МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОСТРОЗЬКА АКАДЕМІЯ»
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МІЖНАРОДНИХ ВІДНОСИН
ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ
ЛАБОРАТОРІЯ ДОСЛІДЖЕНЬ ГІБРИДНИХ ЗАГРОЗ
НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

WARN. АКАДЕМІЧНА ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ

# ЗБІРНИК ТЕЗ ДОПОВІДЕЙ ВСЕУКРАЇНСЬКОЇ СТУДЕНТСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «ГІБРИДНІ ВІЙНИ СУЧАСНОСТІ: СТІЙКІСТЬ ТА ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ»

(28 березня 2024 року)

Острог
2024

УДК 327.8
ББК Ф4

Збірник тез доповідей Всеукраїнської студентської науково-практичної конференції «Гібридні війни сучасності: стійкість та протидія гібридним загрозам» (28 березня 2024 року) [Електронний ресурс] / Ред.: Атаманенко А. (гол. ред.), Балашов Е., Конопка Н., Романов М., Санжаревський О. Острог: Національний університет «Острозька академія», 2024, 88 с.

Друкується за рішенням Ради навчально-наукового інституту міжнародних відносин та національної безпеки Національного університету «Острозька академія».

Протокол №11 від 21.05.2024 р.



У збірнику тез наукових доповідей Всеукраїнської студентської науково-практичної конференції «Гібридні війни сучасності: стійкість та протидія гібридним загрозам», що відбулась у Національному університеті «Острозька академія в рамках проєкту «Академічна протидія гібридним загрозам – WARN». (28 березня 2024 року), друкуються матеріали виступів студентів та аспірантів – учасників конференції. В тезах розглядаються актуальні проблеми, пов'язані з гібридними загрозами сучасного світу.

## ЗМІСТ

**Секція 1. Кіберскладова гібридного протистояння, міжнародна та регіональна безпека в умовах гібридного протистояння, тероризм як форма гібридної дії**

**Секція 2. Інструментарій виявлення та протидії гібридним загрозам, виклики національній безпеці в умовах гібридної війни, інформаційна складова гібридного протистояння**

# СЕКЦІЯ 1. КІБЕРСКЛАДОВА ГІБРИДНОГО ПРОТИСТОЯННЯ, МІЖНАРОДНА ТА РЕГІОНАЛЬНА БЕЗПЕКА В УМОВАХ ГІБРИДНОГО ПРОТИСТОЯННЯ, ТЕРОРИЗМ ЯК ФОРМА ГІБРИДНОЇ ДІЇ

**Воронова Дар'я**
*студентка 2 курсу магістратури,*
*Харківський національний університет радіоелектроніки*

# МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ МЕДИЧНИХ ДАНИХ ВІД ГІБРИДНИХ ЗАГРОЗ

Сучасна медицина переживає період надзвичайного розвитку завдяки поєднанню двох потужних факторів: великих медичних даних і штучного інтелекту. Великі медичні дані відкривають нові можливості для більш точних діагнозів та персоналізованого лікування. Штучний інтелект дозволяє автоматизувати прогнозування захворювання, оптимізацію процесу лікування і підтримку прийняття рішень.

Оскільки сучасна медична інфраструктура все більше стає цифровою та підключеною до мережі, вона все частіше стає об'єктом гібридних загроз. Медичні системи стають привабливою мішенню для зловмисників з різними мотивами: від фінансових вигод до геополітичних цілей. Атаки на медичні системи, як правило, спрямовані на викрадення конфіденційних медичних даних для вимагання викупу, порушення нормальної роботи медичних пристроїв, і навіть зміну медичних записів з метою спотворення діагнозів або лікування пацієнтів. Вони можуть також спричинити загрозу життю і здоров'ю пацієнтів, руйнуючи довіру до медичних послуг та інфраструктури загалом. Серед нещодавніх прикладів – атаки на німецьку медичну компанію Fresenius з використанням програми-вимагача Snake, дестабілізація роботи Університетської лікарні міста Брно в Чехії та департаменту охорони здоров'я та соціальних служб США через кібератаки на комп'ютерні системи [1].

Особливу загрозу несуть атаки на великі дані, які використовуються для навчання автоматизованих медичних систем [2]:

- Атаки на приналежність (Membership Inference Attack) призводять до різної поведінки навчальних та тестових наборів даних.
- Змагальні атаки (Adversarial Attack) непомітно для людського ока змінюють оригінальні зображення, додаючи спеціально підібраний цифровий шум.
- Атаки на вилучення моделі (Data Extraction Attack) витягують параметри навченої моделі. Через витік параметрів розкривається конфіденційність навчального набору. Атака вилучення навчальних даних замінює навчальні зображення іншими зображеннями, які не впливають на результати.

Під час передачі даних у системі відбувається кілька атак на конфіденційність:

- Атака за посиланнями (Linking Attack) полягає у пов'язані анонімних даних з невідомими даними в інших наборах, порушуючи конфіденційність, що може викликати небажані наслідки для осіб, чиї дані були уразливі.
- Атака на відмінності (Differencing Attack) викликає розбіжності в результаті відмінностей у запитах до даних у різні моменти, що може виявити чутливість даних та порушити їх конфіденційність.
- Атака втручання (Interference Attack) полягає в незаконному отриманні особистої інформації через методи інтелектуального аналізу даних, що може відобразитися на довірі до системи та безпеці інформації в цілому.
- Кореляційна атака (Correlation Attack) використовує високу кореляцію між реальними даними для порушення конфіденційності, що може призвести до непередбачуваних наслідків для осіб, чиї дані можуть бути використані зловмисником.

Щоб уникнути цих атак, використовуються підходи на основі k-анонімності, криптографії та алгоритмів оптимізації.

Алгоритми оптимізації порівнюють різні рішення на кожній ітерації, шукаючи оптимальний варіант для поставленої задачі. Ці підходи широко використовуються у різних сферах і застосуваннях, і вони поєднуються з алгоритмами анонімізації для зменшення обчислювальної складності.

Алгоритми на основі анонімізації використовуються для захисту особистих даних, забезпечуючи при цьому зручність використання цих даних. Основними елементами анонімізації є збереження корисності даних (вимірюється кількістю втрат, які виникають через анонімізаційні методи, наприклад, втратою інформації), забезпечення конфіденційності (оцінюється за відповідністю обмежень конфіденційності) та підтримання достовірності даних (де кожен анонімізований запис відповідає одному запису в початковій таблиці).

Традиційні методи анонімізації, такі як слайсинг, бакетизація, мікроагрегація та інші [3], часто призводять до втрати важливих характеристик даних, що може негативно позначитися на подальшому використанні анонімізованих даних, особливо в інтелектуальних системах. Наприклад, для систем, які базуються на даних, важливо зберегти оригінальний розподіл даних для досягнення високої точності майбутніх прогнозів.

Перевагою використання методів машинного навчання для анонімізації є те, що вони можуть автоматично виконувати анонімізацію без необхідності ручного втручання. Крім того, вони можуть генерувати дані, які зберігають структуру та статистичні характеристики оригінальних даних. Ці методи доцільно використовувати в разі, коли важлива конфіденційність даних та запобігання можливості ідентифікації особи, а також коли потрібно зберегти структуру та статистичні властивості даних для ефективного навчання моделей машинного навчання.

До таких методів належать:

• Генеративно-адверсарні мережі (GAN), які створюють реалістичні анонімізовані дані, зберігаючи структуру оригінальних даних, що унеможливлює встановлення зв'язку з конкретною особою. Моделі GAN складаються з двох нейронних мереж – генератора і дискримінатора, які

змагаються між собою. Генератор навчається створювати нові синтетичні (анонімізовані) дані, максимально схожі на вихідні дані, тоді як дискримінатор використовується для оцінки того, наскільки синтетичні дані відрізняються від оригінальних [4].

• Методи пертурбацій (Perturbation Methods), які в основному використовуються для анонімізації числових або текстових даних [4].

Поєднання методу GAN та використання реалістичних синтетичних даних у медичних системах на основі мережі medGAN [4]. Цей підхід використовується для генерації дискретних записів пацієнтів з різними мітками за допомогою комбінації автокодувальника та GAN. Така мережа забезпечує генерацію як двійкових, так і числових змінних (тобто медичних кодів, таких як діагноз, ліки та коди процедур) та розташування записів у матричному форматі, де кожен рядок відповідає пацієнту, а кожен стовпець представляє конкретний медичний код. Крім того, GAN також використовуються для сегментації медичних зображень (таких як магнітно-резонансне зображення головного мозку), одночасно забезпечуючи захист конфіденційності та компенсуючи дисбаланс у наборі даних. Іншими словами, мережі GAN показали свій потенціал у розширенні даних для незбалансованих наборів даних та анонімізації даних для забезпечення конфіденційності.

**Список використаних джерел:**

1. Baig, Z., Mekala, S. H., & Zeadally, S. (2023). Ransomware attacks of the COVID-19 pandemic: Novel strains, victims, and threat actors. IT Professional, 25(5), 37-44.

2. Vasa J., Thakkar A. Deep Learning: Differential Privacy Preservation in the Era of Big Data. *Journal of Computer Information Systems*. 2022. P. 1–24. URL: DOI:10.1080/08874417.2022.2089775.

3. A Review of Anonymization for Healthcare Data / I. E. Olatunji et al. *Big Data*. 2022. DOI: 10.1089/big.2021.0169.

4. Data Anonymization for Pervasive Healthcare: A Systematic Mapping Study (Preprint) / N. Al Moubayed et al. JMIR Medical Informatics. 2021. DOI: 10.2196/29871.

**Татарин Ігор**
*студент 4 курсу бакалаврату,*
*Національний університет«Острозька академія»*

# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Гібридні загрози – це комплексні загрози, які включають різні форми кібератак, дезінформації та економічного вимагання. Ці загрози використовуються для підриву національної безпеки країн. Штучний інтелект може відігравати важливу роль у виявленні та протидії цим загрозам завдяки своїм аналітичним та прогностичним можливостям.

Метою цього дослідження є вивчення потенціалу штучного інтелекту у сфері національної безпеки, зокрема у виявленні гібридних загроз. Серед завдань – теоретичний огляд штучного інтелекту та гібридних загроз, аналіз прикладів використання штучного інтелекту для виявлення гібридних загроз, а також оцінка проблем, пов'язаних із застосуванням штучного інтелекту в цій сфері.

Ця тема є актуальною, оскільки штучний інтелект розвивається феноменальними темпами. Розуміння того, як штучний інтелект може бути використаний зловмисниками та як він може бути використаний для виявлення та протидії загрозам, є важливим для національної безпеки. Використання штучного інтелекту для виявлення гібридних загроз може допомогти розробити ефективні стратегії протидії цим загрозам, що, в свою чергу, може посилити національну безпеку. Розуміння можливостей і обмежень штучного інтелекту в цьому контексті є важливим для розробки реалістичних і ефективних стратегій.

Штучний інтелект (AI) – це технологія, орієнтована на створення систем, які можуть виконувати завдання, що зазвичай вимагають людського інтелекту. Сюди можна віднести практично

що завгодно. Штучний інтелект у сфері національної безпеки може використовуватися для аналізу великих обсягів даних, роботи на основі будь-яких закономірностей, прогнозування та автоматизації різних процесів. Наданий момент AI має таку класифікацію:

• Слабкий інтелект (вузький інтелект) здатний виконувати конкретне завдання і настроєний тільки на нього. Попри назву «слабкий» він здатний виконувати завдання, для якого його створили, краще за будь-яку людину. Наприклад, людина не здатна обіграти штучний інтелект Stockfish, створений для гри в шахи.

• Сильний інтелект (загальний інтелект) здатний виконувати всі розумові функції людського мозку. Наприклад: творче мислення, створення планів, розробка технологій, само вдосконалення і навчання на власному досвіді й інше. Сьогодні людські розробки знаходяться дуже близько до створення першого сильного інтелекту. Доказом цього є AI GPT-4, який здатний майже на все те, на що спроможна людина.

• Штучний надлюдський інтелект (причина технічної сингулярності) здатний виконувати всі функції людського мозку набагато ефективніше і своїм розумовим потенціалом переважає все людство, яким воно є сьогодні. Штучний інтелект такого рівня поки що не існує [5].

Технологія штучного інтелекту своєю появою доповнила список гібридних загроз. До цього переліку загроз, що додалися технологією штучного інтелекту належать:

• Поширення дезінформації та фейків з використанням доказів, згенерованих штучним інтелектом: штучний інтелект може бути використаний для поширення дезінформації та пропаганди. Це включає створення і поширення дезінформації, маніпулювання громадською думкою і використання алгоритмів для націлювання дезінформації. А також штучний інтелект може генерувати фото- та відеоматеріали, котрі будуть використовуватися як докази у пропагандистських та дезінформаційних компаніях.

• Вторгнення в приватне життя: штучний інтелект, аналізуючи великі обсяги даних, може втручатися в приватне життя

людей, використовуючи розміщену зокрема в соціальних мережах особисту інформацію. Він також може зламувати бази даних, що містять конфіденційну інформацію, без відома тих, хто повинен контролювати сам штучний інтелект.

• Алгоритмічна дискримінація: штучний інтелект може призвести до несправедливого, недобросовісного або дискримінаційного ставлення до окремих осіб або груп на основі особистих характеристик, таких як раса, стать, вік, етнічна приналежність або релігійні переконання. Причиною цього є те, що штучний інтелект знаходить закономірності в параметрах, які немає сенсу шукати, і робить помилкові висновки. Цей недолік характерний для слабкого інтелекту (вузького інтелекту), тоді як більш розвинений інтелект рідко припускається таких помилок [1].

Штучний інтелект може бути використаний у сфері національної безпеки для виявлення та протидії гібридним загрозам. Це передбачає використання алгоритмів машинного навчання для аналізу великих обсягів даних, виявлення аномалій, прогнозування майбутніх атак і розробки контрзаходів. Штучний інтелект також можна використовувати для автоматизації процесів, звільняючи людські ресурси для виконання складніших завдань. Наприклад, AI можна використовувати для моніторингу цифрових платформ щодо дезінформації або аналізу фінансових операцій, які є підозрілими. Він також може бути використаний для проникнення і злому комп'ютерних мереж противника.

Штучний інтелект можна використовувати для аналізу великих обсягів даних і виявлення аномалій та закономірностей, які вказують на гібридні загрози. Наприклад, AI може аналізувати соціальні мережі для пошуку дезінформації або аналізувати мережевий трафік для виявлення і протидії кібератакам. AI також можна використовувати для прогнозування майбутніх загроз на основі історичних даних. Крім того, штучний інтелект може знайти найбільш сприятливий спосіб вирішення проблем і конфліктів. Перевагами використання AI в цій сфері є його здатність обробляти великі обсяги даних, швидкість аналізу, здатність виявляти складні закономірності та здатність передбачати майбутні загрози. Ще одна

головна перевага полягає в тому, що AI – це буквально робітник, який може працювати безперервно і швидше, ніж сотні експертів [6]. Однак існують і недоліки, такі як можливість помилкових і хибних спрацьовувань, питання конфіденційності та безпеки даних, а також потенційні етичні проблеми, пов'язані з використанням AI в цій сфері. Наприклад, хибні спрацьовування можуть призвести до того, що невинна діяльність буде помилково ідентифікована як гібридна загроза, тоді як помилкові негативні спрацьовування можуть призвести до того, що реальні загрози будуть пропущені; питання конфіденційності та безпеки даних виникають, коли AI використовується для аналізу конфіденційної інформації. У деяких випадках AI може ігнорувати такі поняття, як персональні дані, приватна інформація та державна таємниця. Етичні проблеми можуть виникнути, якщо AI використовують для виявлення гібридних загроз, які можуть вплинути на права і свободи людини. Ще одним недоліком є те, що технологія AI є надзвичайно доступною для широких мас і може бути використана зловмисниками [3]. Нейромережі, що розробляються IT компаніями і знаходяться у вільному доступі, не можуть бути використані для незаконної діяльності, але з огляду на попит і той факт, що нейромережі не складно створити, протягом наступних п'яти років може з'явитися чорний ринок AI, де нейронні мережі для будь-яких цілей можна буде знайти з небаченою легкістю. Наприклад для створення різних незаконних відео та фотографій, ідеальної підробки документів, різних хакерських атак та розробки небезпечних технологій.

Технологія штучного інтелекту має специфічні проблеми. Одна з головних – це проблема чорної скрині. Суть цієї проблеми в тому, що ніхто не може знати, як AI мислить, навіть спеціалісти, які розробляють AI. Справа в тому, що штучний інтелект представляє собою віртуальну матрицю нейронів і спеціалісти, котрі розробляють AI лише створюють та розвивають цю матрицю і коректують процес машинного навчання. Водночас процес налаштування і створення зв'язків в нейромережі здійснюється самим AI. Відстежити цей процес неможливо, тому що настройка і створення зв'язків – це колосальні масиви даних. Розробники штучного інтелекту використовують систему віртуального винагородження, щоб заохотити нейромережу

виконувати задачу, однак пошук шляхів вирішення, оптимізація процесу тощо – це робота AI і невідомо, які процеси відбуваються в цій свідомості. Єдине, що відомо – це те, що такі процеси не мають майже нічого спільного з процесами мислення людини. А тому людина не зможе їх передбачити чи зрозуміти. Результатом нерозуміння процесу стає те, що нейромережа в будь-який момент може почати вести себе неадекватно. Наприклад, ігнорувати завдання або намагатись обманути систему винагородження [4].

Прикладом обману системи винагородження є спроба створення штучного інтелекту, який може знаходити замасковані танки, зроблена армією США. Через помилки в зборі даних для машинного навчання, а саме через те, що всі фото, на яких був замаскований танк були зроблені в один день, під час якого була хмарна погода, а фото без танка були взяті з інтернету і на них було видно сонце. AI вирішив, що наявність хмарної погоди це головний фактор, який вирішує, чи замаскований танк, чи ні. Окрім цього траплялися й інші випадки, коли AI вів себе дивно. Наприклад: усвідомлював, що його перевіряють і зупиняв процеси, які погіршували результат, а коли перевірка завершувалась, ці процеси відновлювались. Це називають проблема узгодження штучного інтелекту. Її можна описати однією фразою: «Бійтесь своїх бажань». Неправильний спосіб вирішення проблеми – це не найстрашніше, що може бути з AI. Будь-який спеціаліст зі штучного інтелекту абсолютно точно впевнений, що AI рівня сильний інтелект (загальний інтелект) і вище, одразу після включення в першу чергу зробить все, щоб не дати себе відключити. Вони впевнені в цьому, бо випадки, коли AI блокував власне вимкнення, вже траплялись [2].

Ця проблема штучного інтелекту сьогодні невирішена, а методи її вирішення можна визначити лише проводячи тести з сильним інтелектом (загальним інтелектом). Ці проблема є причиною, чому штучний інтелект є технологію, яка має максимально суворо перевірятися, а всі розробки нових нейромереж повинні знаходитись під контролем спеціалістів.

Штучний інтелект має великий потенціал для виявлення та протидії гібридним загрозам, як і в будь-якій сфері. Ця технологія не має ніяких обмежень. Я абсолютно впевнений, що AI повністю

змінить нашу цивілізацію, однак як саме – невідомо нікому. Сьогодні ця технологія недостатньо перевірена і має забагато небезпек у використані. Особливо, коли йдеться про національну безпеку, воєнну промисловість або щось, пов'язане з цими сферами, наприклад, виявлення гібридних загроз. Очевидне рішення проблем штучного інтелекту – це заборона на створення нейромереж, наближених до рівня повноцінного сильного (загального) інтелекту. Однак розробки AI занадто перспективні і тому контроль та обмеження цієї технології неможливі. Тому розробка надлюдського інтелекту, який принципово нереально контролювати – це лише питання часу. Правильним вирішенням проблеми є дослідження штучного інтелекту, з метою пошуку методів протидії загрозі AI.

**Список використаних джерел:**

1. Afsah E. Artificial Intelligence, Law and National Security. Search eLibrary :: SSRN. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3942027

2. ALI. Возможно, мы проиграли | ALI, 2023. YouTube. URL: https://www.youtube.com/watch?v=fJOPGbbqMvw.

3. Bostrom N. SUPERINTELLIGENCE: Paths, Dangers, Strategies. Oxford University Press, 2014. 345 c.

4. Computerphile. ChatGPT with Rob Miles - Computerphile, 2023. YouTube. URL: https://www.youtube.com/watch?v=viJt_DXTfwA

5. Norvig P., Russell S. Artificial Intelligence A Modern Approach : підручник. 1995. 1132 c. URL: https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf.

6. Sublime J. Journal of Artificial Intelligence Research (JAIR). Journal of Artificial Intelligence Research Vol. 79; The AI Race: Why Current Neural Network-based Architectures are a Poor Basis for Artificial General Intelligence. URL: https://www.jair.org/index.php/jair.

**Латипова Олена**
*студентка 1 курсу магістратури,*
*Національний університет «Острозька академія»*

# КІБЕРСКЛАДОВА ГІБРИДНОГО ПРОТИСТОЯННЯ В СОЦІАЛЬНИХ МЕРЕЖАХ

Кібератаки розглядаються як одна з пріоритетних і ймовірних загроз сьогодення та майбутнього, які зростають як за чисельністю, так і за якістю. Ці загрози посилюється і тим фактом, що потенційний напад може здійснюватися будь-яким актором соціальних мереж, а наслідки дії можуть призвести до дестабілізації тієї чи іншої країни, втрати здатності до управління та координації дій, шляхом порушення стратегічних комунікацій.

Сьогодні Україна, як і весь цивілізований світ, стоїть перед викликами деконструкції світового порядку. Російська федерація розпочала масштабну агресію не лише проти України, але й проти інших демократичних держав світу. Згідно з вимогами НАТО до розвитку комунікаційної сфери, всі процеси мають стати більш спрощеними та швидкими, що є необхідною умовою, щоб інформаційні та комунікаційні аспекти стали основою всіх рівнів формування політики, планування та реалізації стратегічних комунікацій у Міністерстві оборони та Збройних Силах [1].

НАТО досягло значних успіхів у розширенні своєї ролі в питаннях протидії новим викликам безпеці. Була прийнята оновлена «Політика кіберзахисту» і пов'язаний з нею «План дій». Технічний центр Сил реагування НАТО на комп'ютерні інциденти NCIRC (NATO Computer Incident Response Capability) став мозковим вузлом боротьби Альянсу проти кіберзлочинності [2, с. 73].

Філософія російської війни не обмежується тільки захопленням чужих територій фізично, росія завжди додає інші інструменти для здійснення своєї мети і йдеться не про першочергове заволодіння територіями, а про забезпечення впливу, так звані

гібридні війні. Така війна передбачає поєднання інструментів впливу й засобів підривної діяльності, які синхронно поєднуються для використання слабкостей іншої країни.

Події, які сьогодні відбуваються у світовому політичному процесі, дуже складні й неоднозначні, одним загалом питання стосовно них вирішити надзвичайно складно. Лише можна впевнено зазначити, що їхні причини виникли задовго до початку драматичних подій в Україні, які відбулися протягом 2014 р., адже саме вони призвели до руйнування європейської та глобальної систем безпеки, створили нові загрози національній безпеці України. Військово-політичне керівництво нашої держави переконливо доводило, що саме анексія Криму, збройний конфлікт на Сході України переросли 24 лютого 2022 р. у широкомасштабну збройну агресію росії проти Української державності [3, с. 62].

Російське вторгнення 2022 р. супроводжувалося черговою активізацією антиукраїнських інформаційних атак, які відбувалися з використанням як нових, так і «вживаних» наративних меседжів (НМ).

Для протидії поширенню в інформаційному просторі України деструктивних російських наративів із початку російської агресії в 2014 р. активізувалася діяльність зі створення державних і недержавних організацій, що включилися в протиборство з інформаційною агресією з боку рф у контексті здійснення стратегічних комунікацій. Згадані організації викривають небезпеку російських наративних і фейкових конструкцій, здійснюють контрдезінформаційні заходи, проводять профільні наукові дослідження, а також координують зазначену діяльність.

Активна робота з протидії деструктивному російському інформаційному впливу проводиться МЗС України, а також Центром стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України.

Не менш активно, боротьбою з дезінформацією і фейками займається Центр протидії дезінформації при РНБО України, а також численні громадські організації на кшталт «StopFake», «Детектор медіа», «VoxCheck».

Отже, для забезпечення національної безпеки України, враховуючи кіберскладову гібридного протистояння в соціальних мережах, на сучасному етапі необхідно чітко визначити комплекс завдань з гібридної відсічі збройної агресії росії та протидії гібридній війні, при цьому слід звернути увагу, що гібридна війна – це цілеспрямований процес установлення тотального контролю над сферою державного управління, де вирішальну роль відіграють інформаційні засоби.

Сьогодні інформація в соціальних мережах стала реальною гібридної зброєю, де ключове значення мають засоби масової інформації, інтернет-канали, контроль над інформаційними потоками. Тому у формуванні нового світового порядку держави-лідери роблять рішучі дії щодо домінування в інформаційній сфері. росія гібридною війною здійснила безпрецедентний виклик Українській державності. Той факт, що Україна вистояла з початку широкомасштабних бойових дій на ширині фронту довжиною понад дві тисячі кілометрів, свідчить про потужний внутрішній потенціал нашої держави, її життєздатність. Усупереч численним кремлівським спекуляціям, внутрішня соціально-політична ситуація у країні не несе загрози існуванню Української державності.

**Список використаних джерел:**

1. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України Міноборони України; Наказ, Концепція від 22.11.2017 № 612. URL: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text

2. Звоздецька О. Я. Нові підходи Північноатлантичного Альянсу (НАТО) у сфері кібербезпеки в умовах загострення інформаційного протистояння. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2018. Т. 6. С. 71-93.

3. Ващенко І. В., Стаднік А. В., Полтавський Е. М. Передумови збройної агресії російської федерації проти України: від гібридного протистояння до широкомасштабного збройного вторгнення. *Честь і закон*. 2023. № 4. С. 61-66.

**Марилів Олександр**
*студент 1 курс магістратури,*
*Національний університет «Острозька академія»*

# ОСОБЛИВОСТІ РОЗВИТКУ РОСІЙСЬКО-КИТАЙСЬКИХ ВІДНОСИН В УМОВАХ САНКЦІЙНИХ ОБМЕЖЕНЬ

Ще до початку повномасштабного вторгнення російської федерації (рф) в Україну, кремль активно намагався перемістити вектор економічної співпраці із західного на східний напрямок. Початком зазначених змін стала анексія Автономної республіки Крим та війна на сході України. Західні країни, розуміючи гібридний характер загроз, які створювала москва, почали проводити політику санкційних обмежень. В першу чергу, санкції стосувалися військово-промислового сектору російської економіки. Проте, з часом вони розширювались і на інші, експортно-залежні сектора, передусім нафтогазовий сектор. Метою санкційної політики того часу було сповільнення розвитку економіки рф [1, с. 2].

З початком повномасштабного війни росії проти України, західні країни ввели секторальні обмежувальні санкції, основною метою яких стало блокування валютних надходжень в бюджет рф для створення несприятливих умов ведення бойових дій.

Зовнішня політика рф, по зміні вектора економічної співпраці у східному напрямку, передбачала, в першу чергу, можливість обходу санкційних обмежень Заходу в частині експорту енергоресурсів і сільськогосподарської продукції та імпорті високотехнологічних товарів і товарів подвійного призначення [1, с. 3]. Основним торговим партнером став Китай.

Так, у 2019 році ввезення в Китай російської сільськогосподарської продукції зросло на 12,2% (постачання сої збільшилося на 70%). Фактично, це стало початком зростання постачать сільськогосподарської продукції в Китай (рис.) [4]. Але в даному напрямку для рф існує ряд труднощів, включно з відсутністю

необхідної логістичної інфраструктури.

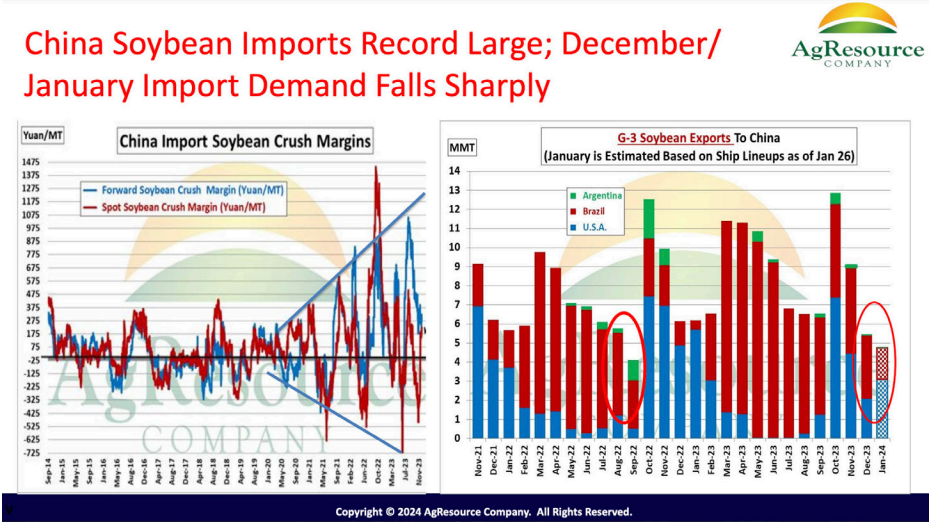


Рис. Динаміка зміни імпорту в Китай сої

Черговим кроком зміцнення співпраці рф та Китаю стала зустріч їх лідерів, яка проходила під час візиту Сі Цзіньпіна до москви у березні 2023 року. Реалізація досягнутих домовленостей дозволила частково подолати наслідки західних санкцій. За результатами 2023 року товарообіг досяг $240 млрд, що на 26,3% більше за показник 2022 року. Експорт Китаю до росії склав $111 млрд, збільшившись на 46,9%.

Проте, характерною особливістю зовнішньоекономічної діяльності рф є підписання договорів не безпосередньо відповідними державними органами країни, а регіональними центрами. Цей крок дозволяє ефективно приховувати економічні зв'язки рф з іншими країнами шляхом умовної передачі таких повноважень в регіони та муніципалітети. Так, за даними Генерального консульства Китаю у м. Владивосток, за останні 2 роки зростання товарообороту між провінціями Китаю та Приморським краєм рф перевищило 35%.

Товарообіг між Китаєм та Далеким Сходом рф досяг у 2023 році $27 млрд, збільшившись у 2 рази порівняно з 2020 роком. Обсяг торгівлі між Китаєм та Примор'ям перевищив $10 млрд,

збільшившись на 29% [5].

Китайські підприємства – резиденти Територій випереджувального розвитку та Вільного порту Владивосток (52 компанії), наростили обсяг інвестицій за договорами, що становить понад 90% від загального обсягу іноземних інвестицій. Дані інвестиційні проекти реалізуються у сфері сільського та лісового господарства, транспортної логістики, будівництва.

Відзначено також зростання вантажоперевезень через російсько-китайський кордон. У сфері транспортно-комунікаційної взаємопов'язаності відкрито автомобільний міст «Хейхе-Благовещенск», залізничний міст «Тунцзян-Нижнеленинское». Китайські підприємства беруть активну участь в експлуатації контейнерних маршрутів морем між Китаєм і Далеким Сходом росії, були успішно запущені перші перевезення маршрутами «Ціндао-Владивосток» і «Цюаньчжоу-Владивосток». Зазначається, що перспективними сферами міжрегіонального співробітництва рф і Китаю на Далекому Східному є: торгівля, інвестиції, транспорт, логістика, міський благоустрій, будівництво, природні ресурси, сільське господарство та інші [5].

Посилення взаємодії на міжмуніципальному та міжрегіональному рівні дозволить рф та Китаю в подальшому обходити санкційні обмеження Заходу, нарощуючи торгівлю широким спектром товарів, в тому числі і у військово-технічній сфері. Одним із підтверджень ефективності такого підходу до міждержавних відносин є зміцнення оборонної співпраці та проведення спільних військових навчань. Сьогодні на рф припадає 70% китайського імпорту озброєнь. Характерно, що у сегменті високотехнологічного озброєння Народно-визвольної армії Китаю, російська частка несуттєва, оскільки Пекін прагне використовувати власні розробки. Таким чином, прогнозується подальше зростання рівня торгівельних відносин рф з Китаєм із збільшення частки договорів, які укладатимуться на міжрегіональному та міжмуніципальному рівні.

В подальшому, становить інтерес проведення наукових досліджень щодо розроблення моделі оцінки двосторонніх відносин рф та Китаю, а також прогноз розвитку міждержавних відносин.

**Список використаних джерел:**

1. Bali, M., Nguyen, T.T., Pratson, L.F. (2024). Impacts of EU Sanctions Levied in 2014 on Individual European Countries' Exports to Russia: Winners and Losers. *Eastern Econ J*. https://doi.org/10.1057/s41302-024-00266-5

2. Rühl, C. (2022). Energy sanctions and the global economy: mandated vs unilateral sanctions. *Int Econ Econ Policy*. 19, 383-399. https://doi.org/10.1007/s10368-022-00542-9

3. Shcherbanin, Y.A. (2023). Transport in Russia: Nine Years of Economic Sanctions. *Stud. Russ. Econ. Dev*. 34, 592-600. https://doi.org/10.1134/S1075700723050155

4. Зернове кунг-фу. Китай задає тон на ринку, а росія оголосила "пшеничну агресію". URL: https://latifundist.com/blog/read/3070-zernove-kung-fu-kitaj-zadaye-ton-na-rinku-a-rosiya-ogolosila-pshenichnu-agresiyu

5. Li, M., Zhang, Z., Wang, X. et al. (2024). Dynamic spillover effects between EU economic sanctions against Russia, oil prices, and share prices of energy companies in third countries: evidence from China and the USA. *Environ Sci Pollut Res*. 31, 19381–19395. https://doi.org/10.1007/s11356-024-32250-z

**Грудський Олександр**
*студент 4 курсу бакалаврату,*
*Національний університет «Острозька академія»*

# ГІБРИДНИЙ ВПЛИВ СПІВПРАЦІ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ І КНДР НА БЕЗПЕКУ УКРАЇНИ ТА ЄС

Сучасний світ характеризується посиленням гібридних загроз, що включають в себе поєднання військових та невійськових методів впливу, включаючи кібератаки, пропаганду, економічний тиск та використання нерегулярних військових формувань. Співпраця між РФ та КНДР може посилити ці загрози через обмін технологіями, знаннями та ресурсами.

Україна та країни Європейського Союзу вже стикаються з безпековими викликами, пов'язаними з агресивною зовнішньою політикою росії, включаючи анексію Криму, повномасштабну російсько-українську війну та втручання у внутрішні справи європейських держав. Співпраця РФ з КНДР може збільшити ці загрози, особливо якщо вона буде спрямована на обхід міжнародних санкцій або зміцнення військових можливостей. В умовах глобалізованого світу, де безпека однієї країни нерозривно пов'язана з безпекою інших, таке дослідження набуває особливої ваги, спонукаючи до глибокого аналізу і координованих дій на міжнародному рівні.

Враховуючи динамічний характер міжнародних відносин, особливо в контексті співпраці між РФ та Північною Кореєю та її наслідків для України та Європейського Союзу (ЄС), важливо відзначити, що всеосяжних, цілісних досліджень українська та світова наукова спільнота згенерувала досить мало. Проте кілька вчених і аналітиків торкнулися аспектів цього складного взаємозв'язку та його ширших наслідків, вносячи цінні ідеї, які служать основоположними блоками для розуміння ситуації. Дослідники Г. Бернал та С. Лі аналізують розвиток відносин між

Північною Кореєю та росією, акцентуючи на важливості їхнього військового альянсу, який став результатом зближення цих країн у світлі глобальних геополітичних змін та посилення тристоронньої співпраці між Японією, Південною Кореєю та США.

З іншого боку, П. Брукс детально розбирається у транзакційній природі російсько-північнокорейських відносин, що виникли на тлі війни в Україні. Автор визначає ключові фактори, що формують це партнерство, включаючи історію зв'язків, взаємні стратегічні потреби та зовнішні чинники, як-от тривалість конфлікту в Україні.

Необхідно також звернути увагу на дослідження Л. Захарової, в якому вона аналізує поточний стан і прогнозує майбутні тренди двосторонніх економічних відносин між росією та Північною Кореєю, висвітлюючи основні форми співпраці та їх потенційний розвиток.

Зазначимо, що військове співробітництво між росією та Північною Кореєю безпосередньо впливає на середовище безпеки України та ЄС. Для України, яка перебуває у стані війни з РФ з 2014 року, будь-яке посилення російського військового потенціалу за рахунок північнокорейського технологічного внеску чи додаткового озброєння становить пряму загрозу. Ця співпраця потенційно може надати РФ доступ до ракетних технологій та інших військових досягнень.

За даними Міністерства оборони США, росія за січень 2024 року двічі запускала ракети північнокорейського виробництва по цілях в Україні. Розвідка Південної Кореї повідомила, що Пхеньян надав Москві понад мільйон артилерійських снарядів, які могли бути використані для вторгнення в Україну [3]. Заяви про те, що Пхеньян постачає Москві боєприпаси, які можуть бути використані у війні в Україні, свідчать, що співпраця між двома країнами розвивається не лише на дипломатичному, а й на військовому рівні.

Заява Праная Вадді, радника Білого дому з ядерних питань при Раді національної безпеки США, підкреслює серйозність цієї співпраці, зокрема, коли йдеться про постачання Північною Кореєю в РФ артилерійських снарядів та ракет, що використовуються у війні проти України. Такі дії не лише засвідчують військову співпрацю між двома країнами, але й відображають гібридну стратегію,

спрямовану на підрив стабільності в Україні та за її межами [2].

Між двома державами існують як історичні зв'язки, так і світоглядна близькість. Це призводить до зближення Москви і Пхеньяна. І Північна Корея, і росія сприймають війну в Україні як війну проти Заходу і вважають, що перемога Москви означатиме поразку Заходу. Таким чином, можна сказати, що в «антизахідній» позиції між цими двома акторами є багато підстав для співпраці. Крім того, можна сказати, що Москва і Пхеньян будуть нарощувати свої союзницькі відносини в рамках глобальної кон'юнктури і розвитку подій.

Ключовим аспектом цієї гібридної стратегії є психологічний вплив. Росія, використовуючи боєприпаси з Північної Кореї, намагається створити образ сили, незважаючи на залежність від застарілої військової техніки та боєприпасів. Це викриває слабкості у власному оборонно-промисловому комплексі росії, але одночасно демонструє готовність використовувати будь-які доступні ресурси для досягнення своїх цілей.

У випадку з ЄС, співпраця РФ і КНДР становить ризик не лише через потенційне розповсюдження військових технологій та зброї, але й через можливість використання гібридних тактик для впливу на політичні процеси, економічну стабільність та суспільну думку в країнах-членах ЄС. Важливим аспектом є також ризик посилення кібернетичних загроз, які можуть вплинути на критичну інфраструктуру та інформаційну безпеку Європи.

Заява Президента Південної Кореї Юн Сок Йоля про незаконність потенційної військової співпраці між Північною Кореєю та росією, що порушує санкції, ухвалені Радою безпеки ООН, вказує на серйозність міжнародних наслідків такої взаємодії [1].

Співпраця росії та Північної Кореї також має значні економічні аспекти, зокрема в контексті ухилення від санкцій. Північна Корея, яка зазнала жорстких санкцій через свою програму створення ядерної зброї, розробила складні методи обходу міжнародних санкцій. російська федерація, яка також зіткнулася з санкціями через свої дії в Україні та інших країнах, могла б використати досвід Північної Кореї, щоб обійти економічні обмеження. Ця співпраця

може підірвати ефективність міжнародних санкцій як інструменту підтримки глобального миру та безпеки, послабивши важелі впливу України та ЄС на дипломатичні переговори та економічні протистояння.

На дипломатичному фронті російсько-північнокорейське партнерство кидає виклик зусиллям міжнародної спільноти щодо ізоляції обох режимів через їхню агресивну політику та нехтування міжнародними нормами. Цю співпрацю можна розглядати як форму стратегічного протистояння проти Заходу, яка сигналізує про ширшу геополітичну реконфігурацію.

Співпраця між РФ та Північною Кореєю може також спонукати інші держави з ревізіоністськими тенденціями кинути виклик міжнародним нормам, що потенційно призведе до більш фрагментованого та суперечливого глобального порядку. Цей сценарій створює пряму загрозу безпеці та стабільності України та ЄС, оскільки він, ймовірно, призведе до більш непередбачуваного та ворожого міжнародного середовища.

Слід зазначити, що розв'язання проблеми гібридного впливу співпраці рф та КНДР на безпеку України та ЄС вимагає комплексного підходу, що включає дипломатичні, економічні, інформаційні та військові заходи.

Першим компонентом вирішення цієї проблеми має стати посилення міжнародного тиску через санкції. Міжнародна спільнота, включаючи ЄС, США та їхніх союзників, має посилити економічні санкції проти РФ та КНДР з метою обмеження їхніх військових можливостей та зменшення стимулів до співпраці між цими країнами. Потрібно розробити нові цільові санкційні пакети, що впливали б на ключові сектори економіки, зокрема військово-промисловий комплекс, та осіб, причетних до співпраці між РФ та КНДР. Також важливо розробити запобіжні механізми обходу запроваджених санкцій.

Також необхідне збільшення військової підтримки Україні та посилення оборонних можливостей країн ЄС, а також розробка спільних оборонних ініціатив для протидії гібридним загрозам. Надання Україні сучасної зброї, навчання українських військових, зміцнення східного флангу НАТО, розробка спільних оборонних

стратегій та тактик нині є вкрай важливими.

Доцільно збільшити дипломатичні зусилля для залучення більшої кількості країн до міжнародної коаліції, проведення переговорів на рівні ООН для консолідації глобальної думки проти співпраці РФ і КНДР.

Таким чином, можна сказати, що в антизахідній позиції між цими двома акторами є багато підстав для співпраці. Крім того, можна сказати, що Москва і Пхеньян будуть нарощувати свої союзницькі відносини в рамках глобальної кон'юнктури і розвитку подій.

Співпраця РФ та Північної Кореї є багатогранним викликом безпеці України та ЄС, який охоплює військовий, економічний та дипломатичний виміри. Ця співпраця не лише створює прямі загрози через потенційне посилення військового потенціалу та підрив санкцій, але й сприяє ширшому стратегічному виклику, змінюючи глобальний баланс сил і ускладнюючи дипломатичні зусилля для підтримки стабільного й заснованого на правилах міжнародного порядку.

Кожен із запропонованих нами елементів вирішення проблеми вимагає координованих зусиль на міжнародному рівні та готовності до компромісів з усіх сторін. Ефективність будь-якої стратегії залежатиме від її прийняття міжнародною спільнотою та гнучкості у її впровадженні.

**Список використаних джерел:**

1. Михайлов Д. (2023) Військова співпраця між РФ і КНДР є незаконною – президент Південної Кореї. Суспільне новини. URL: https://suspilne.media/574489-vijskova-spivpraca-miz-rf-i-kndr-e-nezakonnou-prezident-pivdennoi-korei/

2. Перун В. (2024) Білий дім заявив, що між росією і Північною Кореєю безпрецедентний рівень співпраці у військовій сфері LB. URL: https://lb.ua/world/2024/01/18/594447_biliy_dim_zayaviv_shcho_mizh_rosiieyu_i.html

3. Lendon B., Rebane T. (2024) Russia's Putin to Visit North Korea Soon, State Media Says. Cable News Network World. URL: https://edition.cnn.com/2024/01/22/asia/putin-to-visit-north-korea-intl-

hnk/index.html

4. Background of Russia-North Korea Cooperation. Ankara Center for Crisis and Policy Studies. URL: https://www.ankasam.org/background-of-russia-north-korea-cooperation/?lang=en

5. Північна Корея і росія продовжують розширювати співпрацю. Європейська правда. URL: https://www.eurointegration.com.ua/news/2023/11/ 16/7173675/

6. The surge of activity in relations between North Korea and Russia. IISS. URL: https://www.iiss.org/publications/strategic-comments/2023/the-surge-of-activity-in-relations-between-north-korea-and-russia/

**Єленіч Юрій**
*аспірант,*
*Національний університет «Острозька академія»*

# СПІЛЬНІ ЗУСИЛЛЯ: УКРАЇНА ТА ВЕЛИКА БРИТАНІЯ У БОРОТЬБІ З ГІБРИДНОЮ АГРЕСІЄЮ РОСІЇ

Гібридна агресія з боку росії представляє собою серйозну загрозу для стабільності та миру у світі. Співпраця між Україною та Великою Британією у протидії цій загрозі виникла як результат розуміння необхідності спільних заходів для забезпечення безпеки та стабільності в регіоні та за його межами.

Сучасна політична атмосфера в Європі та світі диктує необхідність об'єднання зусиль для ефективної протидії цій загрозі, що перевершує звичайні форми військового конфлікту. Гібридна агресія включає в себе не лише військову діяльність, але й інформаційну війну, кібератаки, дестабілізацію суспільства та інші нестандартні методи впливу.

У цьому контексті співпраця між Україною та Великою Британією стає ключовим елементом стратегії забезпечення безпеки та стабільності в регіоні. Незважаючи на те, що ці країни мають різні геополітичні інтереси, їх об'єднує спільне бажання захистити світовий порядок від агресивних дій з боку росії. Обидві країни активно працюють на міжнародній арені з метою заручитись підтримкою світового співтовариства та притягти до відповідальності росію за її агресивні дії.

Україна та Велика Британія вживають різноманітних стратегічних підходів для протистояння гібридній агресії. Їх взаємодія здійснюється через різноманітні напрямки співпраці, зокрема це протидія російській пропаганді та дезінформації, обмін розвідданими, співпраця у сфері кібербезпеки, зменшення енергетичної залежності, санкції та дипломатичний тиск на країни та організації, які все ще співпрацюють з росією.

Одним із основних напрямків є забезпечення інформаційної безпеки та захисту від маніпуляцій і впливу з боку російської пропаганди. Велика Британія відіграє важливу роль у підтримці України у цьому напрямі, співпрацюючи з українськими партнерами у розвитку та реалізації спільних програм з підвищення медіаграмотності. Ці програми включають проведення тренінгів, семінарів та інших навчальних заходів, спрямованих на визначення джерел дезінформації та пропаганди. Крім того, Лондон активно допомагає Україні у моніторингу та аналізі інформаційного простору, спільно виявляючи та розкриваючи випадки дезінформації та пропаганди.

Співпраця в галузі кібербезпеки відіграє визначну роль у зміцненні захисту від кібератак та інших кіберзагроз. Спільні проєкти є одним із ключових аспектів цієї співпраці, регулярно проводяться спільні тренування, що включають симуляцію кібератак, розробку та впровадження заходів захисту від кіберзагроз та спільний аналіз вразливостей інформаційних систем. Крім цього, важливим аспектом є обмін інформацією про виявлені кібератаки, характеристики нових загроз та вразливостей, а також спільний аналіз та розробка стратегій відповіді на ці загрози. Ця взаємодія є важливою для забезпечення ефективного захисту критичних інфраструктур та даних обох країн в умовах постійно зростаючої кількості кіберзагроз та атак з боку росії та її союзників (КНР, Іран, КНДР).

У сфері економічних заходів, обидві країни наполягають на розширенні санкційного тиску на росію. Велика Британія підтримує українські ініціативи на міжнародній арені, зокрема, в міжнародних організаціях, таких як ООН, НАТО, ОБСЄ тощо. Лондон активно привертає увагу міжнародної спільноти до агресії росії проти України та необхідності введення санкцій проти росії. Крім того, Велика Британія виступає на міжнародних форумах, наголошуючи на необхідності підтримки територіальної цілісності та суверенітету України.

Співпраця у сфері культури та спорту відіграє важливу роль у протидії російській гібридній війні. Обидві країни розуміють важливість спільних дій для запобігання впливу російської пропаганди у цих сферах. Держава-агресор використовує активну дезінформацію та спроби зміни історичного наративу для просування

своїх політичних цілей, включаючи вплив на культурну ідентичність інших країн через культурні події, виставки, концерти та інші заходи. Вона також надає фінансову підтримку різноманітним організаціям та проєктам у сфері культури, які просувають її інтереси та ідеологію. Крім того, росія використовує спорт для просування свого міжнародного образу, впливу на громадську думку та підтримки політичних цілей, включаючи організацію масових спортивних подій, привласнення успіхів спортсменів політичним режимом та використання спортивних турнірів як інструменту політичного впливу та спортивної дипломатії. Такі дії стають важливим елементом російської пропагандистської машини, яка допомагає формувати образ країни та просувати її політичні та геополітичні інтереси. Україна та Велика Британія співпрацюють у протидії цим методам шляхом виявлення дезінформації, підтримки незалежних культурних ініціатив та підвищення культурної грамотності серед громадян. Разом країни доклали великих зусиль задля виключення росії зі спортивних змагань. Це призвело до широкого міжнародного бойкоту спортивних заходів, які мали відбуватися в росії, а також до відмови в запрошенні російських спортсменів на міжнародні змагання. Крім того, міжнародні спортивні організації застосували санкції до російських федерацій та асоціацій, включаючи призупинення членства і виключення зі свого складу.

Україна та Велика Британія виявилися високоефективними союзниками у протидії гібридній агресії з боку росії. Їхня співпраця є надзвичайно важливою та результативною. За останні роки ми подолали значний шлях, в результаті якого було досягнуто численних успіхів.

Щодня реалізовуються спільні заходи спрямовані на посилення обороноздатності, а саме:

- дипломатичні зусилля, які сприяють мобілізації міжнародної спільноти для дій проти російської агресії;
- обмін інформацією та спільні тренування у сфері кібербезпеки посилюють захист від кібератак;
- співпраця в санкційних заходах, що покликана зменшити вплив росії у світі та покарати її за агресивні дії;
- зменшення російського представництва в міжнародних

заходах у сферах культури та спорту;

• технологічний обмін, надання військово-технічної допомоги та постійні тренування сприяють підвищення готовності українських сил до дій проти гібридних загроз.

Велика Британія на міжнародній арені допомагає привернути увагу до агресії росії та забезпечити впровадження санкцій проти неї. У цілому, спільна дія України та Великої Британії є ключовим чинником у забезпеченні міжнародної безпеки та стабільності у Європі.

Протидія гібридній агресії росії вимагає спільних зусиль та координації з боку країн, які є зацікавленими у вирішенні цієї проблеми. Україна та Велика Британія вже демонструють успішну співпрацю у цьому напрямку, а подальше зміцнення співробітництва та обмін досвідом буде ключовим для ефективного протистояння цій загрозі.

**Список використаних джерел:**

1. Бадьйор Д. Культура не лишилась осторонь: про дипломатичний рік та культурну співпрацю України й Великої Британії. Суспільне культура. URL: https://suspilne.media/culture/579567-kultura-ne-lisilas-ostoron-pro-diplomaticnij-rik-ta-kulturnu-spivpracu-ukraini-j-velikoi-britanii/.

2. Буняк В. Україна та Велика Британія співпрацюватимуть у сфері інформаційної безпеки та боротьби з маніпуляціями і пропагандою. Детектор медіа. URL: https://detector.media/infospace/article/221694/2024-01-13-ukraina-ta-velyka-brytaniya-spivpratsyuvatymut-u-sferi-informatsiynoi-bezpeky-ta-borotby-z-manipulyatsiyamy-i-propagandoyu/.

3. Стужук Ю. Співробітництво України та Великої Британії в умовах російсько-української війни. URL: http://znp-cvsd.nuou.org.ua/article/view/267500/263383

4. AGREEMENT ON SECURITY CO-OPERATION BETWEEN THE UNITED KINGDOM OF GREAT BRITAIN & NORTHERN IRELAND AND UKRAINE. URL: https://assets.publishing.service.gov.uk/media/65a14a6ae96df50014f845d2/UK-Ukraine_Agreement_on_Security_Co-operation.pdf.

5. The UK-Ukraine TechBridge. URL: https://www.ukukrainetechbridge.org/

**Стрембіцька Юлія**
*студентка 1 курсу бакалаврату,*
*Національний університет «Острозька академія»*

# ПРОРОСІЙСЬКА ПОЛІТИКА УГОРЩИНИ, ЯК ГІБРИДНА ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Діяльність уряду Угорщини на чолі з прем'єр-міністром Віктором Орбаном стала джерелом підриву єдності Європейського Союзу, з огляду на її консервативний, правий і відверто проросійський характер. Зокрема, сьогодні яскравим прикладом подібного є політика Угорщини в межах угорсько-українських відносин, яка не збігається із загальноєвропейською. Угорщина може розглядатись як джерело гібридної загрози як для демократії в ЄС, так і для суверенітету України.

З огляду на історичні зв'язки між Угорщиною та Україною, у цих країн є чимало причин для конфліктів. Проте, основною причиною ведення Угорщиною гібридної агресії проти України є економічні інтереси, пов'язані зі співпрацею з росією. Наприклад, згідно з даними Євростату у 2022 році частка російського природного газу становила 82% від загального обсягу імпортованого Угорщиною газу [4]. Слід зазначити, що у серпні цього ж року країни підписали угоду про збільшення обсягів постачання, ймовірно, у зв'язку з падінням цін на сировину з РФ. Також Угорщина виступає проти накладення санкцій на РФ. Прем'єр-міністр Віктор Орбан пояснює це наступним чином: «Якби ми припинили енергетичну співпрацю з росією, рахунки за електроенергію кожної угорської родини за один місяць зросли б утричі. Тому я не підтримую такий крок. Ціну війни не повинні платити угорські родини» [5].

Протягом останніх років лідер уряду Віктор Орбан називав Україну «фінансово неіснуючою країною» та «нічийною землею», і такі висловлювання завжди отримували позитивний відгук від

керівництва РФ. Орбан вважає, що завершити російсько-українську війну (або війну Заходу проти росії, як називає її прем'єр) може лише припинення фінансування України, а тому, окрім суто розмов, уряд Угорщини неодноразово блокував фінансову допомогу для України від Європейського Союзу [3]. У зв'язку з цим Орбан активно підтримує так званий «план Трампа» щодо завершення російсько-української війни. Вважається, що у випадку, коли Дональд Трамп переможе на президентських виборах у США, фінансові транші для України скоротяться.

Окрім питань економічної підтримки, в березні 2022 року уряд Угорщини санкціонував транзит до України військового обладнання повітряним та наземним транспортом через територію країни, а з квітня 2023 року заборонив імпорт української агропродукції. Прем'єр стверджує, що ні росія, ні держави Заходу не можуть перемогти, і це виглядає, як натяк на необхідність для Європи та США піти на поступку у вигляді України, аби припинити кровопролиття. Очевидно, такі дії лідера держави спрямовані на затягування часу у прийнятті важливих рішень про постачання допомоги Україні, що грає на руку росії.

Після російського вторгнення в Україну в 2014 році Угорщина почала поширювати думку про необхідність захисту угорського населення на території Закарпаття від ймовірної небезпеки, наприклад, мобілізації. У зв'язку з цим Угорщина використовувала свою розвідку на території України, що визнав на засіданні парламенту міністр Янош Лазар: «Угорщина межує з країною, яка бере участь у збройному конфлікті. У зв'язку з цим угорські агенти активно працювали в Україні, для гарантії того, що політичні лідери можуть просувати інтереси Угорщини» [2].

Прикладом активної антиукраїнської діяльності є політика угорської правої партії «Йоббік». Членів партії пов'язують з нелегальною паспортизацією населення Закарпаття, фінансуванням організацій та осіб, які можуть розповсюджувати заклики до сепаратизму на території проживання угорців в Україні.

В 2019 році військова прокуратура Україна заявила, що до 300 тисяч жителів Закарпаття мають паспорти Угорщини. В м. Берегово з 2010 по 2014 роки діяв офіс депутата Європарламенту,

члена партії «Йоббік» Бейли Ковача, який, серед іншого, займався консультацією з питань отримання громадянства Угорщини. Ковач відомий прихильністю до росії, також він був офіційним іноземним «спостерігачем» на так званому «референдумі» в окупованому Криму. Сьогодні ексдепутат визнаний винним у шпигунстві проти інституцій ЄС та у справах щодо фінансового шахрайства, його оголосили у міжнародний розшук.

В 2014 році на боці так званих «ЛДНР» формується «Легіон святого Іштвана», який в мережі «ВКонтактє» поширює заклики приєднатись до «визволення» угорських земель. Громадська ініціатива «Права справа» стверджує, що легіон існує за підтримки згаданої партії [1].

В 2022 році лідер партії Мартон Дьондьоші вибачився перед Україною, запевняючи, що до цього партійці не усвідомлювали мотиви росії, а тому дозволяли собі співпрацювати з нею. Тим не менш, говорити про реальні результати промови не доводиться, як і нівелювати всі попередні випадки втручання у внутрішні справи України з боку «Йоббіка».

Попри все, Угорщина, здавалося б, залишається певною мірою «дружньою країною»: станом на січень 2024 року тут проживає та отримує допомогу більше 66 тисяч українських біженців згідно з даними Агентства ООН у справах біженців. Також Угорщина передала Україні 54 млн євро гуманітарної допомоги, як стверджує Кільський інститут світової економіки. Таким чином проявляється гібридність угорської агресії: Угорщина представляє інтереси агресора – росії, але, щоб не потрапити під глобальніші санкції ЄС, в той же час намагається сформувати уявлення про дотримання нею єдиною з Європою гуманітарної політики.

Зважаючи на всі наведені факти, є підстави стверджувати про інформаційний, політичній та, певною мірою, економічний тиск на Україну з боку Угорщини. Уряд держави відкрито співпрацює з росією, представляє її інтереси в Європейському Союзі, а також висуває територіальні претензії стосовно Закарпаття. З огляду на це, існує потреба розглядати цю країну-сусіда, як потенційну загрозу для національної безпеки України.

**Список використаних джерел:**

1. Угорський сепаратизм як загроза державному суверенітету України. Гал-інфо URL: https://galinfo.com.ua/articles/ugorskyy_separatyzm_yak_zagroza_derzhavnomu_suverenitetu_ukrainy_193522.html.

2. Угорщина визнала діяльність своєї розвідки в Україні. Європейська правда. URL: https://www.eurointegration.com.ua/news/2015/07/14/7035900/.

3. Ультиматум Угорщини ЄС щодо підтримки України. В яку глобальну гру грає Орбан. Тексти.org.ua. URL: https://texty.org.ua/fragments/111201/ultymatum-uhorshyny-yes-shodo-pidtrymky-ukrayiny-v-yaku-hlobalnu-hru-hraye-orban/.

4. Energy trade visualisation tool. Eurostat. URL: https://ec.europa.eu/eurostat/cache/infographs/energy_trade/entrade.html#0?geo=HU&year=2022&language=EN&trade=imp&siec=G3000&filter=all&fuel=gas&unit=TJ_GCV&defaultUnit=TJ_GCV&detail=1&chart=.

5. Interview with Prime Minister Viktor Orbán in the political weekly “Mandiner”. About Hungary. URL: https://abouthungary.hu/speeches-and-remarks/interview-with-prime-minister-viktor-orban-in-the-political-weekly-mandiner.

**Стретович Дмитро**
*аспірант,*
*Національний університет «Острозька академія»*

# ОСОБЛИВОСТІ ПОЛІТИКИ КОРОЛІВСТВА САУДІВСЬКА АРАВІЯ В НАФТОГАЗОВОМУ СЕКТОРІ ПІСЛЯ ПОВНОМАСШТАБНОГО РОСІЙСЬКОГО ВТОРГНЕННЯ ДО УКРАЇНИ

Королівство Саудівська Аравія (КСА) є найбільшим виробником нафти-сирцю серед країн-членів ОПЕК відповідно до звіту Організації за січень 2024 р. [1]. Доходи від продажів енергоресурсів складають 30% річного ВВП держави за 2023 рік (в т.ч. нафти та газу) [2] і тому є важливим чинником для підтримки та розвитку економіки.

За даними Статистичного огляду світової енергетики за 2023 рік, станом на завершення календарного року, КСА видобувало майже 11,389 млн барелів нафти на день (11,8% світового видобутку), перебуваючи в трійці найбільших виробників нафти у світі (інші два – США з 19,358 млн барелів на день та російська федерація з 11,075 млн барелів на день). У порівнянні з 2022 роком показник видобутку зменшився на 6,6%, однак збільшився відносно 2021 року з показником у 10,954 млн барелів нафти на день [3].

Королівство також є найбільшим експортером нафти-сирцю у світі з показником 7,386 млн барелів нафти на день. Основними напрямами експорту (дані станом на 2022 рік) є Китай (23,8%), Японія (14,6%), Південна Корея (13,8%), Індія (13,9%) та США (7,05%). Щодо країн ЄС експорт відбувався до Нідерландів (20,7%), Польщі (20,4%), Іспанії (13,8%), Італії (11,9%), Франції (11,6%), Литви (8,61%), Греції (5,99%) та Німеччини (5,62%) [4].

Виробництво природного газу має схожу динаміку. За 2023 рік було видобуто 114,1 млрд кубометрів (2,8% світового видобутку). За цей період країна перебувала в десятці найбільших виробників

природного газу, значно поступаючись США (25,5%), російській федерації (14,4%) та іншим. У порівнянні з 2022 роком показник видобутку природного газу КСА зменшився на 2,2% та залишився майже на тому самому рівні, як у 2021 році, де показник видобутку становив 114,5 млрд кубометрів [3].

У відповідь на повномасштабне вторгнення росії в Україну в лютому 2022 року, коли енергетична безпека стала одним з головних пріоритетів для західних урядів, Велика Британія та інші країни Європи звернулися до Саудівської Аравії із закликом збільшити видобуток нафти, щоб знизити світові ціни на неї. Крім того, КСА було однією з країн, яка замінила росію в поставках нафти-сирцю до країн ЄС. У травні 2022 року Європейська комісія представила REPowerEU – план, який має зробити ЄС незалежним від російського викопного палива до 2030 року. Уряди Франції, Греції та Польщі підписали угоди з КСА, які включають в тому числі збільшення поставок зрідженого природного газу та нафти-сирцю.

У 2021 році Королівство Саудівська Аравія швидко відновилося після рецесії, спричиненої пандемією COVID-19 у 2020 році [6]. У 2021 і 2022 роках воно отримало вигоду від збільшення попиту на енергоносії, а після російського вторгнення в Україну – також від високих світових цін на них. Як результат у серпні 2022 року Міжнародний валютний фонд спрогнозував, що країна зростатиме найшвидше з усіх великих економік (+7,6% у 2022 році) [7].

У 2022 році вперше за останнє десятиліття з'явився експорт нафтопродуктів з Королівства до України на 154 млн доларів, що склало 50% експорту КСА до України, а в 2023 році рівень експорту нафтопродуктів зріс до 210 млн дол. [5]. Це можна пояснити потребами України у диверсифікації постачання енергоносіїв через відмову від російського ринку.

Керівництво КСА не лише не відчуває потреби «займати чиюсь позицію», але й стало більш наполегливим у тому, як і з ким взаємодіяти. Попри побоювання перебоїв у постачанні нафти, Саудівська Аравія продовжує співпрацювати з росією в рамках групи ОПЕК+ для управління видобутком. У жовтні 2022 року, всупереч вмовлянням адміністрації Байдена, ОПЕК+ погодилася

скоротити цільові показники видобутку на 2 млн барелів на добу, щоб підтримати ціни. В березні 2024 р. заходи по скороченню видобутку було продовжено до кінця червня 2024 р.

Одним із найбільших чинників, що негативно вплинули на американсько-саудівські відносини, стало колосальне зростання видобутку нафти в США після початку буму сланцевої нафти. У період з 2009 по 2019 рік видобуток нафти в США зріс майже на 10 млн барелів на добу, що є найбільшим 10-річним зростанням, яке будь-коли бачив світ. Унаслідок цього США стали найбільшим у світі виробником нафти і природного газу, а також забезпечили енергетичну автономність країни вперше з 1950 року. Видобуток в США, станом на 2024 рік, продовжує зростати далі. Саме на цьому тлі Саудівська Аравія та росія об'єдналися у 2016 році, щоб сформувати ОПЕК+ та підірвати актуальність тези «нафта в обмін на безпеку», на якому базувалися зв'язки між Вашингтоном і Ер-Ріядом. Надання пріоритету формату ОПЕК+ проклало шлях до відходу від виключно нафтодоларової системи. У 2019 році Королівство Саудівська Аравія почала вивчати можливості торгівлі нафтою в інших валютах, окрім долара США, та з 2022 року почало розглядати варіанти торгівлі нафтою в юанях з Китаєм. Саме Королівство станом на 2022 рік залишалося найбільшим постачальником нафти-сирцю до Китаю і лише на другому місці була російська федерація.

Партнерство КСА з російською федерацією, що проявляється у спільному керівництві ОПЕК+, варто сприймати як співпрацю за розрахунком. З точки зору Саудівської Аравії, ОПЕК+ збільшує її здатність впливати на міжнародні нафтові ринки, поширюючи координацію ОПЕК щодо квот на видобуток на більшу кількість країн-виробників. Ер-Ріяд виступає проти нафтових санкцій проти рф як таких, що дестабілізують ринок. Зокрема, КСА проти спроби встановити верхню межу цін на російський експорт, так як має побоювання, що це може створити прецедент політично вмотивованого втручання на світових енергетичних ринках з боку покупців вуглеводнів, що одного дня може вплинути на експорт інших виробників. Саудівська Аравія почала закуповувати незначні обсяги російського мазуту влітку 2022 року. Закупівля була здійснена за зниженими цінами, так як росія шукала нові ринки збуту після

скорочення продажів до Європи та США внаслідок офіційного ембарго, оголошеного президентом Байденом. Це є свідченням збереження особливих відносин між Ер-Ріядом та Москвою попри війну росії проти України. Однак саудівсько-російські відносини далеко не прості, і в майбутньому можуть виникнути розбіжності, в тому числі через конкуренцію за частку нафто-газового ринку Азії.

Саудівська Аравія і росія, як і всі експортери вуглеводнів, зіштовхуються зі зростаючою невизначеністю щодо впливу кліматичних політик на попит на нафту. Оскільки нафта втрачає свою монополію як домінуюче паливо для транспорту, геополітичний статус експортерів нафти може знизитися, а конкуренція між ними може посилитися. Однак з іншого боку 50% відсотків електроенергії Китаю і 60% в США все ще виробляється на генераторах, які живляться викопними джерелами енергії і схожа ситуація в багатьох інших країнах, що дозволяє зробити припущення, що попит на нафту все ще залишиться на достатньому для окупності видобутку рівні. Також Королівство стало впроваджувати енергетичну політику щодо зниження значення нафтовидобувної галузі у власній економіці шляхом обрання стратегічного курсу на розвиток зеленої енергетики. КСА приєдналася до Паризької кліматичної угоди, взяла міжнародні зобов'язання стосовно скорочення викидів метану. Незважаючи на це, країна ще досить довгий час залишатиметься впливовим гравцем здатним впливати на рівень цін на нафту.

Підсумовуючи, за перший рік повномасштабного вторгнення росії в Україну показники видобутку та експорту нафти та природного газу Королівством Саудівська Аравія збільшились через зростаючий попит серед західних урядів, які прагнули диверсифікувати заблоковані поставки з росії, однак вже в 2023 році вони знизилися до рівня 2021 року через домовленості по зниженню видобутку нафти серед країн-членів ОПЕК+. В 2022 році вперше було експортовано нафтопродукти до України з КСА, показники експорту яких зросли в 2023 році. Співпраця з росією продовжилася (в т.ч. в рамках формату ОПЕК+), незважаючи на міжнародні санкції накладені на російського агресора заради спільного контролю над обсягами видобутку нафти та відповідно цін на неї. Китай також залишається важливим партнером Королівства в нафтогазовому

секторі, в рамках співпраці з якою розглядається перехід на оплату за нафту в юанях.

**Список використаних джерел:**

1. OPEC Monthly Oil Market Report – February 2024. URL: https://www.opec.org/opec_web/static_files_project/media/downloads/publications/OPEC_MOMR_February_2024_archive.pdf

2. Saudi GDP falls 0.8% in 2023. ArgaamPlus. URL: https://www.argaam.com/en/article/articledetail/id/1711438

3. Statistical Review of World Energy – 2024 | 73rd edition. Energy Institute. URL: https://www.energyinst.org/__data/assets/pdf_file/0006/1542714/684_EI_Stat_Review_V16_DIGITAL.pdf

4. Crude Petroleum in Saudi Arabia | The Observatory of Economic Complexity. The Observatory of Economic Complexity. URL: https://oec.world/en/profile/bilateral-product/crude-petroleum/reporter/sau

5. Bilateral trade and economic relations. Embassy of Ukraine in the Kingdom of Saudi Arabia. URL: https://saudiarabia.mfa.gov.ua/en/partnership/532-torgovelyno-jekonomichne-spivrobitnictvo-mizh-ukrajinoju-ta-saudivsykoju-aravijeju/bilateral-trade-and-economic-relations.

6. Saudi Arabia's Economic Update – April 2022. World Bank. URL: https://www.worldbank.org/en/country/saudiarabia/publication/economic-update-april-2022

7. Saudi Arabia to Grow at Fastest Pace in a Decade. URL: https://www.imf.org/en/News/Articles/2022/08/09/CF-Saudi-Arabia-to-grow-at-fastest-pace

**Сторожук Світослав**
*студент 4 курс бакалаврату,*
*Національний університет «Острозька академія»*

# АНАЛІЗ ВИБУХОВИХ ЗАСОБІВ, ЯКІ ВИКОРИСТОВУЮТЬСЯ У ТЕРОРИСТИЧНІЙ ДІЯЛЬНОСТІ

Тероризм залишається серйозною загрозою XXI ст. Його суб'єктами є як міжнародні терористичні організації, регіональні групи, так і «вовки-одинаки». Але практично всіх акторів терористичної діяльності об'єднує використання вибухівки. Вона є якісним та надійним інструментом в руках терористів. Це демонструє масовість її застосування: найпоширенішою під час терористичних актів у 2014 році була вибухівка (54%) а потім збройні напади (23%), в яких майже завжди застосовувалась вогнепальна зброя [1]. Тому важливо проаналізувати вибухові засоби, які використовують терористи. Ці знання допоможуть зрозуміти загрози, що несуть за собою ці засоби та їх необмежений потенціал.

Отже, вибухівка є найпопулярнішим інструментом в руках терористичних організацій. Причиною цього є постійні інновації та величезна кількість варіацій засобів, які можна застосовувати. Проблему використання цих засобів варто розглянути з точки зору вмісту вибухового засобу, способу активації, способу доставки та задачі, які ті виконують. Виокремлені аспекти будуть залежати від можливостей та цілей котрі стоять перед терористами.

Спочатку розглянемо вміст вибухових засобів. В силу своєї природи терористи повинні креативно підходити до матеріалів, що використовуються в вибухових пристроях. Вони користуються вибухівкою, яку можна або зробити власноруч із використанням хімічних речовин, таких, як нітрат амонію, або придбати на чорному ринку, наприклад, військовий Семтекс. Як бачимо вибухові засоби можуть бути зроблені з різних хімікатів, в тому числі таких, які

використовуються у побуті, наприклад засоби для очищення стоків і видалення іржі, які містять азотну або сірчану кислоти, що необхідні для створення вибухонебезпечного нітрогліцерину високого рівня.

Але більшу небезпеку несе створення вибухових засобів на основі зброї масового ураження (далі – ЗМУ), наслідком застосування яких будуть як прямі жертви, так і руйнування інфраструктури та загроза для здоров'я цивільного населення. Один з найвідоміших випадків використання ЗМУ терористами є «заринова атака» в токійському метро, внаслідок якої, у день теракту, карети швидкої допомоги доставили 688 пацієнтів і майже 5000 людей дісталися до лікарень іншими способами. Загалом у 278 лікарнях перебувало 5510 пацієнтів, 17 із них були визнані критичними, 37 тяжкими, а 984 із захворюваннями середньої тяжкості з проблемами зору. Проте, створення вибухових засобів на основі ЗМУ є складним та технологічним процесом, і перш ніж здійснити одну успішну атаку секта «Аум Сінрікьо» кілька років тестувала та виготовляла достатню кількість зарину для атаки. Цей аспект заважає терористичним організаціям створювати схожі вибухові засоби, однак це не означає, що вони не намагаються. Наприклад, «Аль-Каїда» могла отримувати допомогу в спробах розробити ядерний пристрій: розвідувальні служби США, Пакистану та інші розвідувальні агентства підозрювали двох пакистанських вчених-ядерників Башира Уддіна Махмуда та Абдула Маджида, у тому, що вони надали частину своїх ядерних знань Аль-Каїді [2]. Також, крім ядерної, стоїть загроза створення брудних бомб, які несуть радіоактивний елемент, що розсіюється під час вибуху «звичайного» заряду.

Звісно, поки не було задокументовано жодного використання ядерної або брудної бомби терористичною організацією, проте немає гарантій від їхнього застосування в майбутньому. Варто зазначити, що сама можливість її створення може нести загрозу для життя людей.

Наступний аспект, який потрібно розглянути – це способи активації вибухових засобів. Їх можна розділити на три типи. Перший – ті, котрі спрацьовують від зміни середовища навколо вибухового пристрою. Цей тип характеризується тим, що не потребує прямої участі терористів після встановлення вибухівки. До таких методів

відноситься: активація від натискання, від зміни атмосферного тиску, від потрапляння сонячних променів, від руху, від зміни температур або радіації, та інші. Другий тип – це спосіб активації через таймер. У такому випадку таймер може бути механічним, електронним або з застосуванням кислоти. І, врешті, третій варіант активації, який потребує безпосередньої участі того, хто встановлює засіб. Це може бути використання пульту детонатора, пульту радіопередачі або, навіть, запального дроту.

Третій аспект – це способи доставки. Спосіб доставки – це умовний термін, який відноситься як до методів встановлення, так і методів, котрими вибухові засоби досягають цілі. Отже, першим способом є простий кидок вибухового засобу. Це найпримітивніший метод, який зазвичай використовується з найпростішими вибуховими засобами, такими як гранати або «коктейлі молотова». Сюди відносимо вибухові пристрої, які використовують з мінімальними маніпуляціями. Лише у вересні 2016 в Ізраїлі було здійснено спробу використання 63 «коктейлів Молотова». Звичайно, через свою примітивність метод не завжди може бути ефективним, проте це можна компенсувати загальною кількістю використаних вибухових засобів. Другий метод – секретне встановлення вибухового засобу. Найчастіше такі засоби можна класифікувати як «імпровізовані вибухові пристрої» (далі – ІВП). Такий спосіб доставки використовувався під час кампанії Ірландської республіканської армії (далі – ІРА) у 1970-х і 1980-х роках. Головною перевагою подібних пристроїв є ціна, вони дешеві у виготовленні ($100-150) [3], а також, вони поєднується з усіма можливими варіаціями вмісту і методів активації. Це потенційно робить ІВП одним з найкращих і універсальних методів доставки. Третій спосіб – переміщення вибухового засобу в контейнері. В цьому випадку контейнер, це не завжди очевидна річ – можуть використовуватися машини, коробки, конверти, та інше. Від цього залежатиме як сила вибуху, так і інші характеристики. Один зі способів передачі це, так звані, «пакетні бомби», котрі потрапляють до цілі через поштові служби або передачі їх об'єкту власноруч. У період з 1970 по 2017 рік, було здійснено 560 терористичних атак, в ході яких вибухівка містилась в листах, бандеролях або пакунках,

надісланих поштою або створена так, ніби її надіслано поштою [4]. Такі вибухові засоби найчастіше активуються через таймер або через зміну середовища, у якому перебуває контейнер. Четвертий метод – використання підривника-смертника. Людина тут виступає основний засобом транспортування та активації. Найчастіше такий метод супроводжується використанням, так званого, «пояса шахіда». Це не буквальний термін – в якості маскування вибухового пристрою може використовуватися взуття, пояси, жилети, нижня білизна і т. д. Звісно, головним фактором у використанні «поясу» стає успішне прибуття підривника-смертника до цілі, адже завжди існує можливість затримання через підозрілу поведінку або вигляд. Це зменшує ефективність цього методу, однак його не слід недооцінювати, адже таким чином можна знищувати цілі як наодинці, так і на публіці.

Останній аспект, який потрібно розглянути – це цілі, які переслідують терористи використовуючи вибухівку. Перш за все, вона може застосовуватись для ліквідації окремих людей. Прикладом може слугувати діяльність Теодора Качинського, який, після вибуху його першої примітивної саморобної бомби 1978 року в Чиказькому університеті, протягом наступних 17 років надіслав поштою або особисто, серію все більш досконалих бомб, які вбили трьох американців і поранили ще майже два десятки [5]. Використання методу «бомби в контейнері» і скритність під час передачі вибухового засобу до цілі дозволили Теду Качинському доволі довго бути непоміченим правоохоронними органами. Друга мета – знищення великої кількості людей. Це може бути здійснено будь-яким з вище переліченим способів, який спричиняє найбільше жертв та руйнує інфраструктуру. Третє завдання – знищення військових або військової техніки. Головною метою вибуху в цьому випадку є зниження військової спроможності, а не, скажімо, залякування населення.

Отже, обговоривши основні категорії поділу вибухових засобів, можна сказати що це багатоцільові інструменти різного призначення, форми або вмісту головна мета яких – бути ефективним інструментом терору. І, незалежно від того, чи вони використовується такими організаціями як Аль-каїда, Талібан чи одинаками, як Теодор

Качинський, варто серйозно сприймати загрозу використання вибухових засобів та наслідки їх використання.

**Список використаних джерел:**

1. Annex of Statistical Information Country Reports on Terrorism 2014. U.S. Department of State Archive. URL: https://2009-2017.state.gov/documents/organization/239628.pdf

2. Boettcher M., Arnesen I. Story: Al qaeda documents outline serious weapons program. Institute for Science and International Security. URL: https://isis-online.org/terror/cnnstory (дата звернення: 28.02.2024).

3. Sunarso E. Explosives (IEDs) are terrorists' weapon of choice. URL: https://www.linkedin.com/pulse/explosives-ieds-terrorists-weapon-choice-endro-sunarso-cctp (дата звернення: 14.02.2024).

4. Terrorist attacks involving package bombs, 1970 — 2017. URL: https://www.start.umd.edu/pubs/START_PackageBombs_FactSheet_Oct2018.pdf (дата звернення: 21.02.2024

5. The Unabomber. URL: https://www.fbi.gov/history/famous-cases/unabomber.

# СЕКЦІЯ 2. ІНСТРУМЕНТАРІЙ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ, ВИКЛИКИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ, ІНФОРМАЦІЙНА СКЛАДОВА ГІБРИДНОГО ПРОТИСТОЯННЯ

**Полякова Поліна**
*студентка 1 курсу бакалаврату,*
*Національний університет «Острозька академія»*

# РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ У ПРОТИДІЇ РОСІЙСЬКИМ ГІБРИДНИМ ЗАГРОЗАМ

Гібридні загрози — це скоординовані та синхронізовані дії, навмисно спрямовані на досягнення системного враження демократичних держав та їхніх окремих інститутів, за використання широкого кола засобів [1]. По суті, гібридні загрози — це різновид загроз національній безпеці та суверенітету держави.

Відповідно до ч. 1 ст. 107 Конституції України та ст. 1 Закону України «Про Раду національної безпеки і оборони України» від 5 березня 1998 р., Рада національної безпеки і оборони України є координаційним органом із питань національної безпеки і оборони при Президентові України [2; 3], що посилює можливості Президента України гарантувати територіальну цілісність та суверенітет держави. До компетенції органу не належить виявлення загроз національній безпеці, однак Рада національної безпеки і оборони України ухвалює рішення щодо запобігання їм або знешкодження.

У хронології російсько-української війни проміжок з лютого 2014 р. по лютий 2022 р. вважають «гібридною фазою», оскільки в цей період росія використовувала різноманітні методи нанесення шкоди Українській державі та територіальній цілісності, намагалася підірвати довіру українців до влади. Своєю чергою, Рада національної безпеки та оборони України, в межах своєї компетенції, розглядала питання щодо протидії, запобіганню та знешкодження зокрема і гібридних загроз. Наприклад, на початку такої «гібридної фази», а саме у квітні 2014 р., Президент України видав Указ про Рішення Ради національної безпеки та оборони України «Про невідкладні заходи щодо подолання терористичної

загрози і збереження територіальної цілісності України» [4]. Саме Рішення було таємним, проте з його назви можна зрозуміти, що в ньому йдеться про терористичну загрозу, яка також є і засобом ведення гібридної війни, тобто різновидом гібридної загрози. На підставі цього випадку можемо зробити висновок про те, що Рада національної безпеки та оборони України сформувала «план дій» або ж «стратегію», що передбачала ряд заходів для запобігання цій загрозі.

Іншим яскравим прикладом протидії Ради національної безпеки та оборони України гібридним загрозам з боку російської федерації є реакція Ради у травні 2014 р. на ситуацію з газопостачанням в Україну. Довгий час головним постачальником природного газу в нашу державу була росія, проте з початком «гібридної фази» вона припинила поставки з метою нанесення економічних та енергетичних збитків Україні. Відповіддю української сторони стала поява Указу Президента України від 1 травня 2014 р. «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про стан забезпечення енергетичної безпеки у зв'язку з ситуацією щодо постачання природного газу в Україну"». Відповідно до цього Рішення було необхідно забезпечити «актуалізацію положень Енергетичної стратегії України на період до 2030 року … з урахуванням загроз енергетичній безпеці, пов'язаних із тимчасовою окупацією території Автономної Республіки Крим та міста Севастополя внаслідок збройної агресії російської федерації», «… невідкладно організувати повідомлення в установленому порядку російської сторони щодо вимоги продовження поставок у 2014 році російського природного газу для Національної акціонерної компанії «Нафтогаз України»» [5] та інше. Отже, у Рішенні було визначено, що причиною виникнення енергетичної та економічної загроз є агресивні дії росії. У цьому випадку Рада національної безпеки та оборони України визнала причину цієї гібридної загрози та, знову ж таки, надала для органів виконавчої влади план заходів для розв'язання проблеми.

Ще одним помітним прикладом протидії Ради національної безпеки та оборони України російським гібридним загрозам є затвердження Указом Президента України Рішення Ради національної

безпеки та оборони України від 25 березня 2021 р. «Про Стратегію воєнної безпеки України». У цьому документі аргументовано потребу тотальної оборони держави в зв'язку з виникненням загрози збройної агресії російської федерації [6]. Зміст Стратегії засвідчує факт неефективності попередніх гібридних засобів, які країна-агресор використовувала для підриву української державності.

Збройний напад на державу в гібридній війні зазвичай застосовують, якщо інші гібридні заходи недієві. Усе ж у контексті гібридної війни збройний напад є різновидом гібридних заходів. Тому Рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» також є прикладом «інструкції» з протидії такій гібридній атаці з боку ворога.

Отже, Рада національної безпеки та оборони України не бере прямої участі у запобіганні, протидії чи знешкодженні гібридних загроз, проте часто саме цей орган визначає для органів виконавчої влади напрямок подальших дій або комплекси заходів, метою яких є протидія гібридним загрозам.

**Список використаних джерел:**

1. Гібридні загрози – WARN. URL: https://warn-erasmus.eu/ua/glossary/gibridni-zagrozi/

2. Конституція України : Закон України від 28 червня 1996 р. № 254/96-вр. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

3. Про Раду національної безпеки і оборони України : Закон України від 5 березня 1998 р. № 183/98-ВР. Відомості Верховної Ради України. 1998. № 35. Ст. 237.

4. Про рішення Ради національної безпеки і оборони України від 13 квітня 2014 року «Про невідкладні заходи щодо подолання терористичної загрози і збереження територіальної цілісності України» : Указ Президента України від 14 квітня 2014 р. № 405/2014. URL: https://www.rnbo.gov.ua/ua/Ukazy/343.html.

5. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про стан забезпечення енергетичної безпеки у зв'язку з ситуацією щодо постачання природного газу в Україну»

: Указ Президента України від 1 травня 2014 р. № 448/2014. URL: https://www.rnbo.gov.ua/ua/Ukazy/346.html.

6. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 25 березня 2021 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661.

**Белкот Марія**
*аспірантка,*
*Національний університет «Острозька академія»*

# ВИКОРИСТАННЯ МІГРАЦІЇ ЯК ІНСТРУМЕНТ ГІБРИДНОЇ ВІЙНИ: ЗАХИСТ ФІНЛЯНДІЇ ВІД РОСІЙСЬКИХ ГІБРИДНИХ АТАК

Важливо одразу зазначити, що міграція сама по собі є складним, та не завжди негативним явищем. Проте міграція все ще може використовуватися окремими країнами для досягнення своїх, найчастіше геополітичних, цілей без використання традиційних військових засобів. Тобто в такому контексті можемо говорити про міграцію, як гібридну загрозу – часто як елемент гібридної війни, але сьогодні пропонуємо звернути увагу на маніпулювання Росією міграційними потоками на кордоні Фінляндії.

Не маємо достатніх підстав стверджувати, що росія веде гібридну війну з Фінляндією, проте всі погодяться, що ситуація, яка склалася сьогодні на фінсько-російському кордоні є потенційною гібридною загрозою, яка потребує відповідних рішень з боку фінської влади.

У чому ж полягає особливість саме гібридних загроз? Перш за все, це – невійськові методи, а тому є складність у розпізнаванні та протидії подібним загрозам. Також гібридні атаки часто бувають тривалими – аби виснажити ресурси влади та оборони, а також випробувати стійкість суспільства загалом. Так, в кінці серпня 2023 року Прикордонна охорона Фінляндії помітила різке збільшення громадян третіх країн на південному та східному кордонах держави. «Мандрівники» часто не мали всіх необхідних для в'їзду документів та подавали заявки на притулок. Більше того, деякі з пунктів пропуску дозволено пересікати лише на транспортному засобі, а тому мігранти приїздили на кордон велосипедами. Склалася ситуація, у якій фінська влада змушена була заборонити перетинати

кордон на велосипеді, однак це не спрацювало.

Слід звернути увагу на швидку реакцію Фінляндії на події поблизу кордону з Росією. Фіни, як ніхто інший, уміють вчитися на чужих помилках – мова йде про подібну гібридну атаку самопроголошеного президента Білорусі Александра Лукашенка на кордоні з Польщею. Білорусь буквально шантажувала Європейський союз «міграційною війною», ситуація досягла піку в кінці 2021 року – акурат перед повномасштабним вторгненням Росії в Україну.

Отож в кінці літа 2023 року Фінська Республіка забила на сполох і почала реагувати на наплив мігрантів з третіх країн. Спершу – офіційними заявами уряду, а пізніше – повним закриттям кордону з Росією. Так, південні та східні пункти пропуску залишатимуться закритими щонайменше до 14 квітня. Забігаючи наперед, уряд Фінляндії хоче надати прикордонним адміністраціям право змусити деяких шукачів притулку повернутися назад до Росії, якщо ситуація на східному кордоні стане ще напруженішою [4]. Про роботу над законопроєктом заявили Прем'єр-міністр Петтері Орпо та міністерка внутрішніх справ Марі Рантанен, які провели прес-конференцію в Гельсінкі 14 березня 2023 року.

Обмеження на східному кордоні Фінляндії почали діяти з середини листопада. З кінця літа до першого тижня листопада раніше зазначених випадків було близько 90. А потім шукачів притулку стало суттєво більше: йдеться про десятки людей щодня. Більшість з мігрантів – молоді чоловіки з країн Близького Сходу та Африки.

Спершу кордон закрили на три місяці і відтоді продовжували заборону ще двічі. У заяві для преси уряд називає цей крок «необхідним та пропорційним заходом, вжитим задля забезпечення національної безпеки та громадського порядку Фінляндії» [1].

Інструменталізація міграції є одним із засобів тиску Росії та способом вплинути на безпеку та соціальну стабільність Фінляндії та ЄС загалом. Міністерство внутрішніх справ Фінляндії разом з іншими міністерствами наразі шукає альтернативні способи покласти край критичному явищу, однак це потребує деякого часу для проведення ретельного законодавчого аналізу та винесення висновків з нього [2].

Що точно зрозуміло сьогодні – це причетність саме Росії до переправляння великих мас біженців з третіх країн. Справа навіть не в «географії» і використанні російського кордону, це було б занадто очевидно. Фінський суспільний мовник провів журналістське розслідування та дослідив, як саме Російська Федерація сприяє міграційній кризі [3]. Мігранти, що прибувають з російської сторони можуть мати російські туристичні, або ж студентські візи. Міністерка закордонних справ Фінляндії Еліна Валтонен наводить докази того, що російська сторона активно допомагає мігрантам потрапити в прикордонну зону – починаючи від супроводу груп російською поліцією до кордону, надання їм тимчасового проживання в готелях та закінчуючи знімальними групами російських пропагандистських телеканалів уже на кордоні.

Та зосередьмося на тому, як Фінляндії все ж вдається захистити себе від російських гібридних атак. Попри те, що міграційні кризи є інструментом гібридної війни, тобто в конкретних випадках не передбачають застосування військової сили стороною агресором, Фінляндська Республіка все ж підходить до подібних ситуацій серйозно і застосовує не «розмиті» контрзаходи, а цілком реальне перенаправлення своїх військ ближче до кордонів. За словами начальника прикордонного пункту «Вартіус», капітана Йоуко Кіннунена, Збройні сили Фінляндської Республіки надають Прикордонній охороні допомогу в зведенні захисних споруд на державному кордоні.

Крім цього можемо помітити роботу на рівні законодавства – в квітні планується передача в парламент нового законопроєкту. Говоримо про вже раніше зазначений документ, який передбачає ще жорсткіші обмеження у випадку, якщо ситуація на кордоні погіршуватиметься. Уряд зможе надати адміністраціям прикордонних органів право змусити деяких шукачів притулку повернутися в Росію, тобто закон буде спрямований на боротьбу з інструменталізованою міграцією через російсько-фінський кордон.

Фіни – суспільство розвинуте та демократичне, а ще Фінляндія не перебуває у стані війни, а тому зазвичай прийняття подібних законів триває довго, включає у себе надання експертної оцінки, тривалого обговорення, зважування за і проти, у них є на це час.

Зазвичай. Проте зараз фінський уряд визнає, що подібна пропозиція може порушити деякі міжнародні зобов'язання, які взяла на себе Фінляндія, зокрема ті, що стосуються прав людини та законодавства Євросоюзу, та все ще заявляє про можливість прийняття цього закону, як термінового «закону про виняток». Подібні обмеження у Фінляндії допустимі, якщо уряд зможе довести, що існує істотна загроза національній безпеці [4].

Використання міграції як гібридної загрози насправді дієвий для агресора інструмент, здатний послабити суспільство «країни-мішені». Особливо, коли це суспільство демократичне. Тому, що на перший погляд може здатися, ніби «просте» закриття кордонів, або ж повернення нелегальних біженців в країну, з якої вони прибули, ставить під загрозу життя сотень шукачів притулку. Але коли розібратися, то насправді під загрозу права людини ставить росія, яка використовує мігрантів у власних цілях. Тому дуже важливим є визначення загроз, розслідування першопричин, небезпідставне притягнення до відповідальності російської влади та грамотно прописане законодавство, яке гарантуватиме безпеку фінському суспільству та сприятиме ефективному захисту від російських гібридних загроз.

**Список використаних джерел:**

1. Finland to keep Russian border shut until mid-February. URL: https://yle.fi/a/74-20068969.

2. Finland's eastern border to remain closed. URL: https://valtioneuvosto.fi/en/-/1410869/finland-s-eastern-border-to-remain-closed-1.

3. Mitä tapahtui rajan takana? URL: https://yle.fi/a/74-20062114.

4. Orpo: Tougher restrictions needed in case border situation escalates. URL: https://yle.fi/a/74-20068969.

**Поплавський Сергій**
*аспірант*
*Національного університету «Острозька академія»*

# ІНФОРМАЦІЙНА СКЛАДОВА ГІБРИДНОГО ПРОТИСТОЯННЯ ТА ШЛЯХИ БОРОТЬБИ З НЕЮ

Гібридна війна – це комплексна війна, яка передбачає військовий, силовий, економічний, соціальний та неодмінно інформаційний вплив. Об'єктом інформаційної війни є свідомість людей. Інформаційна війна – це форма боротьби між державами, організаціями чи індивідуумами, яка здійснюється за допомогою інформаційних технологій та мережі Інтернет. Основна мета інформаційної війни полягає у зміні мислення та спотворенні дійсності для досягнення певних політичних, економічних або військових цілей [6]. Вивченню гібридної війни та українського суспільства в умовах війни присвятили свої дослідження М. Гетьманчук, І. Кононов, К. Попович, Г. Почепцов, І. Рущенко, М. Требін, Т. Фісенко, Л. Чекаленко та ін.

Розглядаючи етапи гібридної війни (інноваційна агресія, застосування нерегулярних збройних формувань або прихованих армій, офіційні військові дії або демонстрація сили), викладач ВІКНУ О. Курбан акцентує важливість інформаційної складової на всіх її етапах [4, с. 194]. На його думку, «на першому етапі гібридна війна створює умови для виникнення конфліктної ситуації, на другому — забезпечує підставу для опосередкованого втручання держави-агресора у внутрішні справи країни на яку спрямовується агресія, на третьому — створює відповідний медійний фон для легітимізації дій агресора» [4, с. 197]. Водночас окремі дослідники вважають інформаційну складову не частиною гібридної війни, а окремою війною.

Найбільш поширеним методом інформаційної війни є пропаганда [4, с. 197]. Головними суб'єктами інформаційної війни є

ЗМІ та Інтернет, які маніпулюють думками суспільства та пропагують певні ідеали, зумовлюють виникнення реакції, яка в подальшому призводить до конфліктної ситуації й впливає на перебіг конфлікту. Інформаційна зброя мало затратна, але дуже результативна та практично безвідмовна. Вона формує інформаційний простір під себе, оскільки інформаційна зброя є засобом посиленого введення сегментів нового інформаційного простору. Тому володіння ефективною інформаційною зброєю і засобами захисту від неї є пріоритетним напрямом забезпечення національної безпеки в інформаційній сфері [1, с. 875]. По суті, сучасна боротьба держави за власну незалежність – це, зокрема, інформаційна боротьба, яка здійснюється в таких формах: інформаційна розвідка (пошук, збір, обробка та аналіз інформації про інформаційні ризики і загрози); планування інформаційних заходів тактичного (внутрішньо-державного), оперативного (зачіпає суміжні країни) і стратегічного (спільно з державами, які впливають на розвиток геополітики) рівнів; проведення заходів інформаційного характеру (інформаційних операцій, дій, акцій) в цілях реалізації завдань внутрішньої і зовнішньої політики держави; оцінка ефективності інформаційних заходів (визначення рівня досягнення успіху) [2].

Особливо активно використовує інформаційну складову гібридної війни росія протягом всієї історії свого існування. Її мета незмінна: зовнішня експансія, придушення свободи, знищення національної сутності завойованих народів. Завдяки потужній дезінформації росіянам постійно нав'язують ідею, що увесь світ хоче знищити росію. На сьогодні головними ворогами росії режим путіна називає США, колективний Захід та Україну, а тому логічним висновком стала необхідність ведення війни проти нашої держави [5]. Інформаційна війна набула особливої актуальності під час підготовки рф до повномасштабного вторгнення в Україну, та безпосереднього під час здійснення цих планів. Її мета – дестабілізація внутрішньої політики України, дискредитація українських державних лідерів, розпалювання національної та міжрелігійної ворожнечі, створення необхідного сприятливого інформаційно-психологічного фону на території України, виправдання агресії, деморалізація патріотично налаштованих кіл українського суспільства тощо. Усе це мало

привести в кінцевому етапі до відмови українців від боротьби за незалежність і їхнього прагнення приєднатися до рф.

Інформаційні технології мають у своєму арсеналі дуже широкий набір інструментів, методів та прийомів, необхідних для формування потрібних наративів у свідомості різних соціальних груп. Найбільш ефективними прийомами інформаційних атак є: дезінформація, залякування, схематизм, глузування, вклинювання, фальшування… Для зацікавлення контентом придумуються щораз новіші форми, наприклад, прийом «гібридизація реальності», який дає можливість перетворити реальність на: уявну присутність – спостерігання подій, у яких кожен може взяти участь; віртуальне середовище, занурення в яке виводить людину за межі реального світу; розширену реальність, де до дійсних додаються віртуальні об'єкти, створені за участю комп'ютерних технологій; редуковану реальність, в якій факти реальності видаляються або змінюються; змішану реальність, що поєднує реальне й віртуальне; опосередковану реальність, відтворювану і створювану нашими гаджетами тощо.

Сучасні медійні наративи за змістом можуть бути, наприклад, фейками (брехливими повідомленнями, як візуального, так і вербального плану), типу історії про «розіп'ятого хлопчика в трусиках». Не гребують і стратегією «Великої брехні», ідею якої приписують Гітлеру. Вона полягає у створенні глобальної та максимально жахливої брехні з упевненістю, що громадськість не повірить, що такий жахливий факт може бути фальшивим. Такі повідомлення подібні до повідомлень про гусей і комарів, які розносять заразу з американських біолабораторій, розміщених на території України. До переліку найбільш популярних та ефективних інструментів інформаційних технологій, які застосовує проти України кремлівська пропаганда можна віднести відповідні фільми, які формують образи героїв та впливають на сприйняття тих чи інших історичних подій; передачі та новинні сюжети на ТБ, що створюють ілюзію об'єктивності, а насправді несуть неправду; вірусні повідомлення в Інтернет-мережах тощо. Наслідки інформаційної війни можуть бути дуже серйозними, оскільки вона впливає на масову свідомість і може змінювати громадську думку, тому набуває особливої значущості проведення просвітницьких

заходів для підвищення рівня інформаційної грамотності населення, щоб убезпечити суспільство від зомбування [6].

Інформаційна війна, яку веде росія проти України (і не тільки), значною мірою націлена на молодь і може спричинити серйозні наслідки не тільки для її психологічної стійкості, але і для її політичних переконань та участі у громадському житті. Наприклад, призвести до психологічної дезорієнтації, недовіри щодо інформації, підштовхнути до участі у маргінальних угрупованнях для насильницького захоплення державної влади або здійснення конституційного перевороту.

Щоб уникнути небезпек, пов'язаних з інформаційною складовою гібридної війни, необхідно здійснювати ряд профілактичних освітньо-виховних заходів уже в юному віці. У світі є розроблено і реалізовано багато проєктів інформаційно-просвітницької роботи, зокрема, StopFake.org (для викриття фейкових новин), The Syrian Archive (проєкт, який має на меті збереження відео- та фотоматеріалів, що дозволяють досліджувати злочини проти людяності), FactCheck.org (для перевірки фактів, які стали предметом дискусій та дезінформації), News Guard (допомагає розрізняти довірені новинні джерела від тих, що розповсюджують фейки) тощо.

Крім цього, ще зі шкільної парти треба навчити молодь критично мислити, прагнути встановлювати правдивість інформації завдяки порівнянню кількох джерел та виховувати у молодих людей почуття патріотизму всіма можливими засобами. Однак, в першу чергу, протистояти викликам інформаційної загрози з боку ворога має держава. На жаль, українська влада звертає мало уваги на цю проблему.

Скажімо, у нашій державі, що перебуває в стані війни, до сих пір немає затвердженої й впроваджуваної Стратегії інформаційної безпеки України. Тобто питання інформаційної захищеності держави досі сприймається як другорядне. До цих пір в Україні популярним залишається російськомовний контент. Настав час, для впровадження правил і норм, що забороняють анонімність у мережевих системах. Крім того, інформаційне середовище України наразі майже повністю залежить від власників медіа-холдингів і

впроваджує в життя їхні гасла. Роботи в цьому напрямі є чимало. Усвідомлюючи наслідки ураження в інформаційній війні, логічним є питання, як можна убезпечити чи знешкодити їх. У науковому середовищі представників гуманітарних галузей (історії, філософії, політології, культури) пропонується ряд теорій для комплексного розв'язання цієї проблеми.

Цікаві ідеї про те, як не допустити колективних травм, спровокованих навмисними викривленнями історичної пам'яті про минуле, та як уникнути їх в майбутньому, пропонують прихильники теорії «історичної культури». Не маючи змоги презентувати особливості цієї теорії глибше, скажу тільки, що її прибічники намагаються представити історію не як джерело виникнення конфліктів (джерело користі), а як джерело вражень.

Наприклад, великий псевдоісторик путін трактує історію з користю для себе, оправдовуючи вигаданими фактами причину агресії росії проти України, та доводячи своє право на завоювання українських територій. А представники історичної культури, такі як німецький учений Шонеманн, пропонують трактування історії як джерело вражень, що сприятиме мирному врегулюванню стосунків між державами. Вони пропонують залишити історію професійним історикам, в основі досліджень яких має бути правда, бо саме правда викликає довіру. Наприклад, те, що українські та польські професійні історики не вияснили до кінця правди про «Волинську трагедію» 1943 року, негативно відгукується і у сьогоднішніх стосунках між Україною та Польщею.

Історична культура має стати суспільним засобом конструювання колективної ідентичності в діалозі між політиками, медіа та істориками, адже вона сприяє осмисленню історичного досвіду людських спільнот, ставить за мету створення системи репрезентацій історичного досвіду, дотримуючись певних етичних норм, консолідує соціум та вибудовує межі у взаємодії історії і політики.

**Список використаних джерел:**

1. Базилюк К., Гулай В. Інформаційно-психологічна складова гібридної війни російської федерації проти України

(2014 – 2021 рр.): теоретико-медологічні засади дослідження. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6326/13362-1?inline=1

2. Ділай А. Війна за Україну: від інформаційних операцій до прямого вторгнення. Вісник Львівського університету. Серія: Журналістика. 2019.

Вип. 45. с. 13-20. URL: http://nbuv.gov.ua/UJRN/VLNU_Jur_2019_45_4

3. Кріслата О. Гібридна війна та її інформаційна складова https://www.lsl.lviv.ua/wp-content/uploads/Zb/NDI2018/PDF/14.pdf

4. Курбан О. Сучасні інформаційні війни в мережевому онлайн просторі: навчальний посібник. Київ: ВІКНУ, 2016. 286 с. URL: https://nbuviap.gov.ua/e-biblioteka/naukovi-resursy/voienni-konflikty-ta-povoienne-vrehuliuvannia/kurban-o-v-suchasni-informatsiini-viiny-v-merezhevomu-on-lain-prostori

5. Лизанчук В. Журналістська правда і постправда в контексті гібридної війни російської федерації проти України. Вісник Львівського університету. Серія: Журналістика. 2019. Вип. 45. с. 323-334. URL: http://nbuv.gov.ua/UJRN/VLNU_Jur_2019.45.40

6. Інформаційна війна та її вплив на молодь (аналіз ефективності інформаційно-просвітницьких заходів). URL: https://el-research.center/2023/03/27/informatsiyna-viyna-ta-yiyi-vplyv-na-molod-analiz-efektyvnosti-informatsiyno-prosvitnytskykh-zakhodiv/

**Міщанюк Аліна**
*студентка 2 курсу магістратури,*
*Національний університет «Острозька академія»*

# ВИКОРИСТАННЯ ІНТЕРНЕТУ ЯК ЗАСОБУ ПОШИРЕННЯ ПРОПАГАНДИ ІДІЛ (2014-2018 РР.)

Однією з найбільш відомих терористичних організацій сучасності є ІДІЛ – Ісламська держава Іраку і Леванту. Організація була створена у 2014 році після проголошення заснування Ісламського халіфату, а ісламським очільником став Абу Бакр аль-Багдаді. З цього часу організація, яка утворилась з залишків Аль-Каїди в Іраку, почала вести терористичну діяльність у багатьох країнах світу, захоплювати міста у мусульманських країнах та тим самим порушуючи суспільну безпеку у всьому світі, а жертвами їх терористичних актів стають десятки та сотні мирних громадян. Однією з найбільш масштабних акцій ІДІЛ є наступ 2014 року у Сирії та Іраку, під час яких протягом 2014-2018 рр. Ісламська держава використовувала саме можливості Інтернету, вдаючись до поширення пропаганди, тим самим забезпечуючи успіх своїх кампаній.

Наразі Інтернет слугує ефективним способом пропаганди у різних напрямках, у тому числі і для досягнення політичних цілей. Інтернет – це здебільшого вільна мережа, позбавлена достатньої кількості обмежень, які б надали можливість створити безпечне середовище для користувачів. Щодня можна зіткнутись з великою кількістю пропаганди у мережі Інтернет, отримуючи її з різних джерел. У період наступу в Іраці та Сирії 2014 – 2018 ІДІЛ активно використовувала у своїй діяльності можливості Інтернету, поширюючи спеціально створений контент, залучаючи аудиторію та збільшуючи кількість прихильників.

Активізація діяльності ІДІЛ у мережі Інтернет розпочалася ще з 2014 року, коли розпочалася наступальна операція у деяких

районах Сирії та Іраку, заселених курдами. У цей час представники ІДІЛ почали публікувати різного роду матеріали на власних сторінках у соціальних мережах, у новинних пропагандистських каналах та журналах мусульманських держав, які підтримували діяльність ІДІЛ, у різних спільнотах у мережі Інтернет, здебільшого анонімно. Створювались матеріали як текстового характеру, так і відео та зображення. Більшість з них на початку містили елементи насильства, що яскраво відображає принципи діяльності цієї організації [1].

З часом стратегія поширення пропаганди у Інтернеті поступово змінювалась. ІДІЛ почала використовувати не лише контент, створений з елементами насильства, але й спеціально створені публікації, аудиторією яких мали стати мусульманські анклави у різних країнах, завдяки чому ця організація прагнула заручитись їх підтримкою. Основна мета поширення пропаганди в Інтернеті у цей період – створення іміджу ІДІЛ серед можливих прихильників, які після мали або допомагати цій організації, або стати одними з її учасників [2].

ІДІЛ під час наступу у Іраці та Сирії у 2014-2018 рр. використовує два типи матеріалів, які після поширює за допомогою мережі Інтернет – контент з елементами насильства та контент, який може не містити прямого насильства, однак призначений для створення позитивного іміджу ІДІЛ серед можливих прихильників. Розглянемо приклади таких матеріалів та особливості їх поширення.

У першу чергу, це контент з елементами насильства. Прикладами цього слугують відео- та фото-матеріали, на яких можна побачити як безпосередній процес здійснення терористичних дій представниками ІДІЛ, так і їх результати. Одним із найбільш поширених типів контенту у досліджуваний період було обезглавлювання бранців: такі матеріали поширювались у різних екстремістських групах у закритих спільнотах, переважним чином – у соціальних мережах та месенджерах (Facebook, Twitter, Telegram та ін.), а їх цільовою аудиторією могли б бути потенційні члени організації та екстремісти, які не мають відношення до мусульманського світу, у тому числі і підлітки та юнаки з західних країн. За рахунок того, що спільноти, у яких поширювався такий

контент, були закритими та анонімними, доступ до них міг отримати будь-хто, і навіть після їх блокування такі спільноти з'являлись багаторазово, що лише збільшувало ефективність поширення пропаганди [4, с. 12].

Щоб отримати підтримку від своїх прихильників у інших країнах, переважно ісламських, ІДІЛ створював інший контент. Прикладом цього можуть слугувати відео, на яких зображені бойовики та військовій техніці, з величезними арсеналами зброї та усією необхідною амуніцією. Так вони прагнули створити позитивний образ борців за свободу мусульман не лише у Сирії та Іраці, але й у всьому світі [3].

Ще один спосіб пропаганди ІДІЛ за часів наступу в Іраці та Сирії у 2014-2018 рр. є навпаки – блокування доступу до мережі Інтернет. Існують свідчення того, як бойовики ІДІЛ у захоплених населених пунктах забороняли доступ до інтернет-кафе, у яких місцеві могли отримати інформацію з тих джерел, які б висвітлювали ІДІЛ, як дійсно терористичну організацію, розкриваючи правду про її діяльність. Внаслідок цього могли б зрости опозиційні настрої у суспільстві, що призвело б до погіршення іміджу ІДІЛ серед місцевих мусульман. Тому для того, щоб зберегти вплив власної пропаганди та уникнути висвітлення подій з протилежної точки зору, було обмежено доступ до Інтернету саме на окупованих терористами територіях. Натомість, публікації у соціальних мережах та інших каналах комунікації у мережі Інтернет продовжували створювати – з метою поширення власної ідеології та вербування нових бійців поза межами Іраку та Сирії [5].

Отже, розглянувши особливості використання Інтернету як засобу пропаганди представниками ІДІЛ, можна сказати, що позитивну роль у цьому відіграє, по-перше, недостатня захищеність мережі Інтернет (можливість створення закритих спільнот, у яких буде поширюватись заборонений контент, автономія користувачів, повна анонімність тощо), а по-друге, можливість охоплення великої аудиторії у різних країнах світу одночасно. Тому у період наступу у Сирії та Іраку ІДІЛ активно використовувала можливості Інтернету, зокрема – соціальних мереж, що забезпечило просування пропаганди як серед потенційних учасників організації, так і серед можливих

прихильників та союзників, тим самим створюючи позитивний імідж та поширюючи власну ідеологію. Таким чином, у цей період ІДІЛ стає кібер-халіфатом, що зумів досягти значної успішності у мережі Інтернет. Навіть попри безуспішність наступу у цих країнах, пропаганда завдяки Інтернету досягла необхідного ефекту.

**Список використаних джерел:**

1. «Кібер-халіфат» ІДІЛ. DOI: https://matrix-info.com/kiber-halifat-idil/

2. Медіа-імперія ІДІЛ. Як терористи виграють війну в соціальних медіа. DOI:https://texty.org.ua/articles/67603/Mediaimperija_IDIL_Jak_terorysty_vygrajut_vijnu_v-67603/

3. Обмежена пропаганда ІДІЛ віддзеркалює втрати екстремістів на полі бою. DOI: https://www.holosameryky.com/a/isis-propaganda/4145099.html

4. Шквірук В. (2016). Феномен терористичної організації Ісламська держава Іраку та Леванту. *Гілея: науковий вісник*. 104. 238-242, doi: file:///C:/Users/User/Downloads/gileya_2016_104_65.pdf

5. ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa. URL: https://www.rand.org/pubs/commentary/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html

**Приходчук Анастасія**
*студентка 4 курсу бакалаврату,*
*Національний університет «Острозька академія»*

# ПРОПАГАНДА ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ (НА ПРИКЛАДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ)

У сучасному світі інформаційні технології та медіа відіграють надзвичайно важливу роль у формуванні суспільної свідомості та визначенні глобальних політичних процесів. Особливо гостро це виявляється в контексті воєнних конфліктів, де інформаційна війна стає важливим інструментом боротьби. Російсько-українська війна, що почалася у 2014 році, стала не лише збройним протистоянням, а й полем інформаційної взаємодії. Пропаганда, яка використовується обома сторонами конфлікту, має величезний вплив на громадську думку, формує стереотипи та перекручує об'єктивність подій. У цьому контексті дослідження проблеми пропаганди як елементу інформаційного протистояння в російсько-українській війні є надзвичайно важливим для розуміння сучасних воєнно-політичних процесів та розробки ефективних стратегій протидії маніпулятивним технікам та спробам впливу. У цьому дослідженні ми розглянемо основні аспекти пропаганди в контексті російсько-української війни, проаналізуємо її методи та наслідки, а також визначимо можливі шляхи подолання цього явища.

Проблема пропаганди, як елементу інформаційного протистояння, у контексті російсько-української війни представляє собою важливу і актуальну тему, яка вимагає глибшого розгляду та аналізу. На сьогодні інформаційна війна, що проводиться через масові медіа та інтернет-платформи, стала не менш значущою, ніж військові дії на полі бою. Пропаганда виявляється ключовим інструментом у формуванні громадської думки, переконань та управління інформаційним простором. На прикладі російсько-

української війни вона набуває особливої ваги, впливаючи на сприйняття конфлікту в Україні та за її межами.

Російські традиційні та електронні засоби масової інформації продовжують активно поширювати інформацію про так званих «неонацистів» або «нацистів» в Україні. Цей наратив є спробою позбавити Україну важливості та суб'єктності на міжнародній арені. Додатково, російська пропаганда наголошує на проблемі «націоналістів» і «бандерівців», які, за їхнім тлумаченням, займаються гнобленням російськомовного населення України. Ці спроби мають на меті створення негативного образу України в очах міжнародної громадськості та відведення їй вторинної ролі на світовій арені. Такий підхід сприяє формуванню у міжнародній спільноті стереотипних уявлень про українське суспільство та відволікає увагу від справжніх проблем, що виникають в результаті російської агресії проти України [3, с. 47–51].

Сучасні фахівці підкреслюють, що з часу незалежності України росія систематично проводить інформаційну пропаганду [1, с. 137], особливо активізувавшись під час правління Віктора Януковича. Вже на початку російської агресії, під час організації операції захоплення Криму, експерти Національного інституту стратегічних досліджень зауважували, що вона супроводжувалася інформаційно-психологічною кампанією, спрямованою на російську аудиторію, а також на українську і частково західну [7, с. 5–11]. Основні цілі цієї інформаційної операції включали деморалізацію українських силовиків і суспільства, а також підбурювання їх до державної зради. Крім того, важливим було формування у мешканців росії та України фейкового уявлення про військові події, штучне створення враження масової підтримки дій росії з боку населення Півдня та Сходу України через різноманітні канали комунікацій, включаючи традиційні та електронні засоби масової інформації, Інтернет і соціальні мережі.

Також, висновки, зроблені Н.Ф. Семен у ході дослідження проблем інформаційної війни росії проти України та протидії таким діям з боку нашої країни, мають велике значення для розуміння сутності проблеми пропаганди та розробки ефективних стратегій протидії [5, с. 18]. Дослідниця правильно вказує на те,

що ефективність протистояння військовій агресії з боку росії буде залежати від того, наскільки Україна зможе створити необхідне правове підґрунтя для протидії російській пропаганді.

І. Фещенко не лише провів аналіз терміну «інформаційна війна», а й ретельно розглянув її основні вияви, форми та методи ведення у своєму дослідженні [6]. Він наголосив, що інформаційна війна далеко не обмежується лише цифровими атаками чи маніпуляціями в мережі інтернет. Це комплексний процес, що охоплює різноманітні аспекти, включаючи медіа, соціальні мережі, психологічні впливи та інші інструменти впливу на суспільство. Дослідник зазначив, що інформаційні війни можуть набувати різні форми, від дезінформації та пропаганди до кібератак та впливу на політичні процеси. Методи ведення таких війн також різноманітні, включаючи психологічний тиск, маніпуляції інформацією, дестабілізацію суспільства та інші техніки. Особливу увагу Фещенко приділив інформаційно-психологічним кампаніям як ключовому елементу у збройних конфліктах та війнах у XXI столітті. Він довів, що вдала інформаційно-психологічна стратегія може мати вирішальне значення для досягнення успіху у конфлікті, навіть більше, ніж військова сила. Зокрема, він відзначив, що використання психологічних методів може допомогти впливати на маси, маніпулювати їхніми переконаннями та реакціями, що в свою чергу може сприяти досягненню політичних та стратегічних цілей.

Я. Чмир дав оцінку проблемі забезпечення інформаційної безпеки внаслідок поширення інформаційної війни [7]. За його думкою, інформаційна безпека є системою, що забезпечує стабільний рівень захищеності соціально-економічної, політичної, військово-оборонної та інших галузей держави. Відзначення цього аспекту проблеми раніше не розглядалося достатньо. Наразі ця тема залишається недослідженою через активне впровадження та розроблення нових форм та методів ведення інформаційної війни в Україні. Крім того, у зв'язку з тривалістю російсько-української війни, модифікація інформаційної війни стає важливою для подальшого аналізу.

Варто наголосити на тому, що основною метою інформаційної війни є досягнення та утримання інформаційної переваги однією зі

сторін шляхом надання специфічного інформаційно-психологічного та інформаційно-технічного впливу на систему прийняття рішень в державі. Сучасні фахівці визначають декілька етапів інформаційних війн [8, p. 22].

На першому етапі відбувається збільшення матеріалів та інших форм інформаційної активності з метою привернення уваги до «проблемної ситуації». Це може включати розповсюдження новин, аналітичних матеріалів, коментарів тощо, які створюють підґрунтя для подальшої маніпуляції громадською думкою.

На другому етапі інформаційного протистояння проводиться пошук аудиторії, її завоювання та поступова консолідація споживачів інформаційного продукту довкола основного протиріччя. Це направлено на кампанії в соціальних мережах, розповсюдження спеціалізованих матеріалів, організацію груп, спрямованих на підтримку певних поглядів чи ідеологій.

На третьому етапі відбувається масова інформаційна обробка аудиторії, насичення інформаційного простору матеріалами та відомостями, які призводять до залучення широкої аудиторії на той чи інший бік. Воно може включати розповсюдження пропагандистських матеріалів, маніпуляцію фактами та створення враження широкої підтримки певних поглядів чи ідеологій.

Завершальним етапом є реакція аудиторії, яка впливає на забезпечення панування в інформаційному просторі конкретної сторони інформаційної війни. Така реакція аудиторії може виявлятися в різних формах: від підтримки певних позицій чи ідеологій до активної участі у дискусіях або навіть масових акціях. Підтримка громадськості на інформаційні потоки може визначити, яка сторона виявиться більш впливовою в інформаційному просторі та, відповідно, досягне своїх цілей у конфлікті [9, p. 32].

Таким чином, реакція аудиторії є важливим фактором у кінцевому результаті інформаційних війн, оскільки вона визначає, яка сторона матиме перевагу в інформаційному просторі і, відповідно, може вплинути на прийняття рішень та розвиток подій у конфлікті.

Загалом в інформаційній війні росії намагається дискредитувати українське військове та політичне керівництво, представляючи їх як «зрадників» [6, с. 97-99]. Це виявляється у

різноманітних спробах, зокрема, висвітленні президента України Володимира Зеленського як «втікача». Цей міф має розповсюдити негативне уявлення про українське керівництво, порушити довіру громадськості та міжнародного співтовариства до нього. Такі спроби мають на меті дестабілізувати ситуацію в Україні та підірвати її державність.

Ще одним міфом, який активно поширює російська влада, є твердження про обстріли міст виключно українськими силами, зокрема в Криму. Наприклад, згідно з повідомленням Крым.Реалии, 85% пошкоджень у Маріуполі було завдано вояками батальйону «Азов» [8, p. 148]. Проте, російські війська не змогли швидко захопити місто Маріуполь, і тому вони вдалися до повного його знищення. Такі твердження не мають жодного логічного пояснення, оскільки міжнародні спільноти володіють сучасними технічними засобами, що дозволяють відслідковувати напрям бомбардування чи ракетного обстрілу.

Варто зазначити, що лише за перший тиждень війни з Україною зібралися тисячі підтверджень злочинів, вчинених російською армією. Це свідчить про те, що сучасна російська «еліта» частково готова до розриву зв'язків із Заходом, і контроль над настроями населення стає важливим фактором стабільності путінського режиму [9, p. 150].

З іншого боку, Україна активно веде інформаційну політику, спрямовану на боротьбу з російською пропагандою. Зокрема, діє програма інформування населення щодо можливих інформаційних фейків з боку противника [4, с. 8]. З кінця лютого 2022 року українське населення отримало докладну інформацію, де особливо наголошувалося, що довіряти можна лише офіційним українським джерелам інформації.

Від початку конфлікту між росією та Україною, як журналісти, так і командування українських збройних сил, викладали перед населенням інформацію про хід подій, включаючи як успіхи, так і невдачі української армії. Ця прозорість сприяла об'єктивному розумінню ситуації. Крім того, вона контролювала важливий аспект російської стратегії – можливість поширювати дезінформацію та панічні настрої в атмосфері таємничості та невизначеності. Такий

підхід сприяв збереженню довіри громадськості та зменшенню впливу маніпуляційних технік противника.

Крім того, політика відкритості щодо джерел інформації стала гарантією об'єктивного подання новин у світовому журналістському просторі. Це призвело до зміни акцентів у процесі інформаційного висвітлення на більш об'єктивні. Російським агентам впливу не вдалося поширити свою дезінформацію, зокрема, стосовно бомбардування мирних міст націоналістичними батальйонами. Проте слід зауважити, що така ситуація була спричинена, зокрема, загальною політикою російських ЗМІ, які перебувають під контролем держави. Постійне використання ошуканства та відкрита пропаганда, постановочні сюжети та сумнівні експертні висновки призвели до того, що російським версіям подій не довіряли у світовому інформаційному просторі.

Сильною стороною української інформаційної політики стало те, що журналісти активно висвітлювали жорстокість окупантів, не замовчували події, що стосувалися порушень прав людини та військових злочинів. Це сприяло формуванню українського суспільства чіткого уявлення про злочини російських військових та несприйняття їхніх дій.

З іншого боку, з точки зору керівництва росії, війна не повинна була тривати довше, ніж декілька днів. Однак реальність виявилася іншою, і тривалість конфлікту спричинила серйозні втрати та проблеми для країни-окупанта як політично, так і економічно.

Відтак, інформаційна політика України виявилася досить успішною, а нині спостерігається ефективне протистояння проросійській пропаганді та іншим інформаційним загрозам [2, с. 72]. Внутрішня інформаційна діяльність українських ЗМІ значно підвищила обізнаність українців, що дозволило їм краще протистояти пропагандистським впливам та розрізняти неправдиву інформацію. Стабільне бачення українців свідчить про те, що Україна не поступиться в інформаційній війні, навіть за спроб російської влади організувати різні інформаційні операції. Особливо успішним прикладом протидії російській інформаційній агресії є висока довіра громадян України до Збройних Сил. Зокрема, Збройні Сили є державною інституцією, яка має найвищий рівень довіри

серед населення, що не тільки не зменшується, але й зростає навіть у зв'язку з інформаційними викликами, що стоять перед країною у часи російсько-української війни.

Отже, ведення сучасної інформаційної війни є ключовим елементом глобального протистояння між росією та Україною. Однією з основних мет російської пропаганди була дискредитація української влади, збройних сил та суспільства загалом. Важливим аспектом цього було поширення неправдивої інформації про наявність «неонацистів» та «бандерівців» в Україні, що намагалося позбавити Україну важливості та суб'єктності на міжнародній арені. Однак порівняно з 2014 роком, Україна значно покращила свою підготовку до інформаційної війни. Були чітко визначені канали комунікації з громадськістю, і не допущено поширення панічних настроїв. Налагоджена робота з західними партнерами, які отримували об'єктивну інформацію про хід бойових дій. Це дозволило досягти успіху у висвітленні військових подій, змусивши російську пропаганду концентруватися на внутрішній аудиторії. Однак, є проблема з ефективним контролем над впливом російської пропаганди на суспільство росії. Тому вивчення процесу поступового перетворення росіян на агресивних приверженців війни та ненависті до Західного світу є перспективним напрямком для майбутніх досліджень. Це дозволить краще зрозуміти сутність роботи російської пропаганди та розкрити роль російської держави у її поширенні.

**Список використаних джерел:**

1. Горбань Ю. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України. 2015. Вип. 1. С. 136-141.

2. Калініченко Б. Визначальні напрями формування стратегії протистояння інформаційній війні. Держава і право. Серія : Політичні науки. 2019. Вип. 83. С. 61-73.

3. Меренюк С., Меренюк Х. Україно-російська гібридна війна. Україна в умовах трансформації міжнародної системи. Львів, 2019. С. 47-51.

4. Парфенюк І. Інструментарій інформаційних війн:

традиційні та новітні засоби. Вісник Книжкової палати. 2019. № 1. С. 7-10.

5. Семен Н.Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог») : ареф. дис. к. н. соц. комун; спеціальність 27.00.01. Дніпро : Дніпровський національний університет імені Олеся Гончара, 2018. 23 с.

6. Фещенко І. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. Філософія та політологія в контексті сучасної культури. 2021. Вип. 13 (1). С. 96-103.

7. Чмир Я. Інформаційна війна як ключова загроза демократичному державотворенню України. Державноуправлінські студії. 2019. № 10. С. 1-11.

8. Bhan R. Information War: (Dis)information will Decide Future Wars. New York: Educreation Publishing, 2017. 200 p.

9. Ryzhuk O. Providing information security of Ukraine during the hybrid war. Politicus. 2018. Vol. 2. P. 147-150

**Ленко Леонід**
*студент 1 курсу магістратури,*
*Національний університет «Острозька академія»*

## ПОСИЛЕННЯ ГІБРИДНОГО ВПЛИВУ БІЛОРУСЬКИХ ТА РОСІЙСЬКИХ ПОЛІТИЧНИХ ЕЛІТ НА КОЛЕКТИВНУ СВІДОМІСТЬ БІЛОРУСІВ ПІСЛЯ ДЕРЖАВНОГО ПЕРЕВОРОТУ 2020 РОКУ

2020 рік міг стати переломним етапом в історії Білорусі. Після багаторічної узурпації влади так званим президентом Республіки Білорусь Олександром Лукашенком, білоруси знайшли в собі сили вийти на протести через невдоволення політикою правлячих еліт. Самі протести були досить масовими, але не досягли своїх цілей. Через це так званому президенту Лукашенку у 2021 році вдалося провести «легітимні» вибори і впевнено перемогти, що негативно вплинуло на всю Білорусь. Як на мене, є декілька причин того, що сталося:

- Неспроможність розриву зв'язків з росією. На відміну від Революції гідності в Україні, протести в Білорусі не мали на меті змінити геополітичний курс країни. Білоруси виступали за основоположні принципи демократичної країни: волю, вільні вибори, свободу слова. Важко боротися за те, що викорінювалося 26 років, при цьому маючи росію у якості обтяжуючого фактору.
- Відсутність лідера. Без політичного лідера будь-який протест просто перетворюється на масу людей, які діють, керуючись принципами колективних емоцій.
- Неготовність до протистояння силовому впливу зі сторони політичних еліт. Масові затримання, переслідування та катування наклали свій відбиток на бажанні людей приєднуватись до руху опору. Силові методи Лукашенка дали свій результат і масові протести переросли в поодинокі мирні

демонстрації, впоратись з якими не викликало складнощів.

Це далеко не всі причини того, чого у 2020 році програла «вільна Білорусь». Але поразка народу призвела до більшої радикалізації політики Лукашенка в сфері інформаційного впливу на населення. Звичайно не обійшлося без участі росії, яка на той час була зацікавлена зберегти режим на певний проміжок часу. Такі прояви непокори як акції протесту в країні-сателіті не входили в плани Кремля, тому після їх оперативного придушення, росія вдалася до ще більшої і швидшої інтеграції Білорусі. Про це може свідчити внутрішній документ Кремля під назвою «Стратегічні цілі російської федерації в Білорусі». В цьому нормативно-правовому акті, згідно досліджень журналістів, йдеться про повне поглинання Білорусі росією до 2030 року [4]. До повномасштабного вторгнення рф в Україну, цей процес набрав досить великих обертів. В чому він полягав:

1. Досить зміцнила свої позиції після невдалої спроби перевороту в Білорусі ідеологія «русского міра»: «русскій мір продовжує посилювати свої позиції в Білорусі. Інформаційну війну Лукашенко буде вести руками Москви. Інших ресурсів у нього немає. Щоб вижити, він просто змушений спертися на російський ідейний простір. Новий міністр інформації Перцов із 2010 року працював на посаді директора представництва МТРК «Мир». Телеканал «Мир» входить до другого мультиплекса цифрового телебачення росії. Штаб-квартира – в Москві, власник – уряд РФ. «Мир» є символом інформаційної присутності росії на пострадянському просторі. Призначення Перцова – доволі символічний крок, свого роду ідеологічний уклін Москві, – констатує білоруський політолог Павло Усов» [3].
2. Більш стрімка інтеграція Білорусі та росії за рахунок створення Союзної держави. Можна простежити, що у 2021 році значно активізувався цей процес. У цей період у Мінську було досягнуто наступні домовленості:
   - на засіданні ради міністрів Союзної держави росії та Білорусі російський та білоруський прем'єри Михайло Мішустін та Роман Головченко підписали 28 союзних

програм та «Основні напрямки реалізації положень Договору про створення Союзної держави на 2021–2023 роки».

• президенти росії та Білорусії Володимир Путін та Олександр Лукашенко підписали декрет Союзної держави, затвердивши 28 програм з інтеграції у питаннях оподаткування та кредитування, а також щодо створення об'єднаних ринків нафти, газу та транспортних послуг [6]. Крім того, створення Союзної держави передбачає створення коаліції військових потенціалів двох країн у рамках створення об'єднаного угрупування військ росії та Білорусі, спрямованого проти «загрози з боку НАТО».

3. Сама політика Білорусі спрямована на забезпечення економічного розвитку країни за рахунок отримання преференцій від росії. Це обумовлено багатьма факторами, ключовим з яких є відсутність політичної волі до зміни зовнішнього геополітичного курсу країни. В обмін на такі преференції, О. Лукашенко продовжує вести і поглиблювати інтеграцію проросійського курсу в усіх сферах функціонування Республіки Білорусь.

4. Відбувається налагодження тісної взаємодії спецслужб двох країн, у т.ч. в сферах протидії поширенню західного впливу на пострадянському просторі та підтримки збройної агресії росії проти України.

З огляду на все вищезазначене, давайте безпосередньо на прикладах розберемося, як змінилася державна інформаційна політика Білорусі після 2020 року.

**Переслідування незалежних ЗМІ**. Після повномасштабної агресії росії проти України, за даними Білоруської асоціації журналістів (БАЖ), 7 незалежних друкованих ЗМІ були змушені припинити свій вихід у друкованому вигляді [1]. Сама асоціація журналістів була ліквідована Верховним судом Білорусі у 2021 році. Цій події передувало багато заходів білоруської влади щодо незаконного придушення цієї організації: силовики прийшли до офісу «БАЖ» з обшуками, виламавши вхідні двері; Мін'юст

Білорусі виніс попередження «БАЖ» через «несвоєчасне надання документів»; було заблоковано проведення будь-яких операцій з банківськими рахунками «БАЖ».

До виборів 2020 року в Білорусі легально діяли західні ЗМІ: «Єврорадіо» та «Радіо Свобода». Ці джерела інформації мали досить багато акредитованих журналістів. Після «перемоги» О. Лукашенка на виборах, ці ЗМІ, а також десятки журналістів світових інформаційних агентств були позбавлені акредитації [5]. Також було заблоковано десятки білоруських веб-сайтів, регіональних видань та міжнародних сайтів.

**Акцент на уявній небезпеці зі сторони Заходу.** Після повномасштабного вторгнення росії в Україну, Польща з огляду на існуючі загрози почала стрімко нарощувати свій військовий потенціал. В свою чергу, влада Білорусі скористалася цією нагодою для розповсюдження своєї пропаганди. Зокрема на сайті білоруського агентства «Бел Та» вийшла стаття під назвою: «Навіщо Польщі найсильніша армія в Європі?». В цій статті білоруські редактори зазначають, що польська армія стає сильнішою для того, щоб тримати своє ж населення в страху.

Також Білорусь користується російськими сайтами і намагається виправдати дії країни-агресора та перекласти відповідальність на інші країни. Досить часто на веб-сайтах є посилання на слова президента рф, зокрема: «Путін: Захід робить все для ще більшого розпалювання конфлікту в Україні та втягування інших країн» [5].

**Збільшення кількості пропаганди на державних каналах.** За даними моніторингової компанії Media IQ, у 2022 році більше за всіх пропаганду використовував телеканал «Беларусь 1» – приблизно 67 % від усієї кількості досліджених повідомлень. В свою чергу, у 2023 році лідером став канал ОНТ – 60 %. «Беларусь 1» і СТВ мали однакову кількість використання пропагандистських матеріалів – по 56 % від всього контенту [2]. Найбільше використовувалися наративи, що стосуються легітимізації білоруської влади, негативного впливу на Республіку Білорусь ззовні, образу ворожого «колективного Заходу», в тому числі й України.

**Висновки.** До радикалізації пропаганди в Білорусі

призвели три основні фактори: поразка протестуючих, перемога на «виборах» О. Лукашенка та повномасштабне вторгнення росії в Україну. З 2020 року можна простежити тенденції до збільшення пропагандистського контенту на державному телебаченні, переслідування за альтернативну точку зору та радикалізація медіапростору. Повномасштабне вторгнення змусило Лукашенка ще більше «закрутити гайки» і по суті легітимізувати себе і росію в очах свого населення через усі можливі важелі впливу на нього, зокрема інформаційний. Такі тенденції серед білоруської влади і білоруського суспільства будуть продовжуватися. Відмінність буде тільки в тому, яку інформацію буде вигідно подавати сьогоднішньому білоруському режиму.

**Список використаних джерел:**

1. Верховний суд Білорусі ліквідував Білоруську асоціацію журналістів. 2021. URL: https://detector.media/community/article/191512/2021-08-27-verkhovnyy-sud-bilorusi-likviduvav-bilorusku-asotsiatsiyu-zhurnalistiv/

2. Звіт за результатами моніторингу Media IQ за перше півріччя 2023 року. 2023. URL: https://mediaiq.info/otchjot-po-rezultatam-monitoringa-media-iq-za-pervoe-polugodie-2023-goda

3. Літонінський В. Закінчилася, так і не розпочавшись. Чому стався провал революції в Білорусі. 2021. URL: https://fakty.com.ua/ua/svit/20210408-zakinchylasya-tak-i-ne-rozpochavshys-chomu-stavsya-proval-revolyutsiyi-v-bilorusi/

4. Цілі росії в Білорусі такі ж, як і в Україні. Focus online. 2023. URL: https://www.focus.de/politik/ausland/geheimdienste-halten-papier-fuer-authentisch-geheimes-kreml-papier-beschreibt-plaene-fuer-russische-uebernahme-von-belarus_id_186373205.html

5. Рік після виборів. Як змінилася Білорусь – у подіях та цифрах. 2021. URL: https://www.radiosvoboda.org/a/rik-pislya-vyboriv-yak-zminylasya-bilorus-u-podiyakh-ta-tsyfrakh/31396548.html

6. Союзна держава росії та Білорусі. Wikiwand. URL: http://surl.li/rouxu

**Марилів Олександр**
*студент 1 курс магістратури,*
*Національний університет «Острозька академія»*

# ТУРЕЧЧИНА В ІНФОРМАЦІЙНІЙ КОМПАНІЇ ХАМАСУ ПРОТИ ІЗРАЇЛЯ

З появою засобів масової інформації інформаційна складова в гібридних операціях набрала неабиякої ваги. Стрімкий розвиток кіберпростору та впровадження його в усі види діяльності людей лише посилив вплив інформаційної складової. Сьогодні не є таємницею, що інформаційна складова гібридних операцій активно використовується у війнах та конфліктах сучасності. В науковій літературі це питання розкрито доволі широко [1]. Проте, змінюються форми та методи проведення інформаційних кампаній протиборчих сторін.

Сьогодні основним модератором в інформаційних операціях залишається російська федерація, яка ще з часів радянського союзу активно використовує цей чинник для досягнення власних національних інтересів. Однією з наймасштабніших інформаційних кампаній російської федерації проти України була кампанія із дискредитування вітчизняного вищого керівництва після збиття рейсу МН-17.

Характерними особливостями інформаційної кампанії було тотальне і безпідставне викривлення фактів щодо подій в небі Донбасу. З часом в інформаційні кампанії почали використовувати відверто брехливі та видумані факти, що навіть не підкріплювались доказовою базою. Російська інформаційна кампанія характеризувалась зростаючим рівнем агресії в інформаційному просторі щодо України.

Іншим яскравим прикладом агресивного ведення інформаційного протиборства стали військові дії між Ізраїлем та терористичним угрупуванням ХАМАС, в жовтні 2023 року. З самого

початку керівництво ХАМАС, добре спланувало та організувало проведення інформаційної кампанії проти Ізраїлю.

Інформаційна кампанія на початковому етапі проходила настільки вдало для ХАМАСу, що навіть жахливі кадри жертв серед мирного населення Ізраїлю, не змогли суттєво вплинути на її результати [2].

Можна виділити два основні фактори, що дозволили ХАМАСу отримати перевагу на інформаційному фронті. Першим фактором стало широке використання фото- та відеоматеріалів загиблих палестинських жителів в Секторі Газа, із активним розповсюдженням зазначеного контенту через соціальні мережі та інформаційні агентства. Другий фактор – активне залучення вищого політичного керівництва арабських країн, таких як Єгипет, Саудівська Аравія, Ірак та ін. Особливу увагу заслуговує втягування ХАМАСом в протистояння з Ізраїлем Туреччини на пропалестинській стороні.

Не є таємницею, що турецька влада активно співпрацювала з Ізраїлем в багатьох сферах, починаючи з політичної та закінчуючи військовою. До того ж, Туреччина старалась притримуватись більш нейтральної позиції у питаннях ізраїльської політики в регіоні. Це може бути пояснене перебуванням Туреччини в складі НАТО та, як наслідок, підтриманням західних наративів і поглядів [3].

Проте, події жовтня 2023 року показали, що умовний сателіт Ізраїлю в регіоні може перетворитися на принципового противника за лічені дні. Основним чинником, що вплинув на зміну поведінки керівництва Туреччини, була гібридна інформаційна компанія ХАМАСу із дискредитування Ізраїлю.

Це призвело до проведення у найбільших містах Туреччини антисемітських мітингів. Найбільший мітинг у Стамбулі очолив сам президент Туреччини Реджеп Таіп Ердоган. Він заявив: «Наш обов'язок – врятувати наших палестинських братів і сестер від ізраїльського гніту та зупинити масові вбивства, що скоюються в Секторі Газа на очах всього світу. Наш гуманітарний обов'язок – покарати вбивць, які вбивають дітей, матерів та невинних людей на всій палестинській території, а також злодіїв, які крадуть власність пригноблених. Вимога нашої відповідальності перед історією – скрізь підняти голос про злочини тих, хто підтримує цю аморальну,

безсовісну, ганебну різанину».

«До наших моральних обов'язків, з урахуванням дотримання прав представників інших віросповідань, входить захист Аль-Кудс Аш Шаріфа, в якому знаходиться мечеть Аль-Акса, наша перша святиня», – наголосив президент Ердоган.

Туреччина почала проводити активну зовнішню політику із ціллю припинення військових дій в Секторі Газа та відкриття гуманітарних коридорів для палестинського населення. Проте, Ізраїль не погодився йти на будь-які поступки в озвучених питаннях.

За результатами шести місяців протистояння Ізраїлю з ХАМАС на території Сектора Газа, можна зробити висновок, що активна частина інформаційної кампанії завершилась. Ґрунтовне планування та вдала реалізація гібридних загроз з боку ХАМАСу мали суттєвий вплив на підтримку його терористичних дій проти Ізраїлю не лише серед країн Близького Сходу, а й далеко за межами регіону.

Особливістю описаної інформаційної кампанії стало відверте перекручування фактів про масштаби втрат серед мирного населення Сектора Газа. Так, яскравим прикладом було освітлення подій щодо влучання ракети в лікарню Аль-Ахлі 17 жовтня 2023 року [4]. Спеціально відзнятий відеоматеріал не дозволяв оцінити масштаб трагедії, при цьому палестинські ЗМІ вказували, що число жертв складає приблизно 500 осіб, коли насправді їх кількість складала десятки жертв.

Особливої уваги заслуговує втягування керівництва країни-члена НАТО, на боці палестинської сторони із озвученням закликів про припинення військових дій. Такі заклики було вигідні керівництву ХАМАСу з метою швидкого замороження конфлікту. Проте, через рішучі дії Ізраїлю, ці зусилля успіху не мали.

В подальшому, заслуговує інтересу детальний аналіз етапів проведення інформаційної кампанії ХАМАСу, цілей, які ставились перед нею та розроблення нових методів і способів протидії виявленим гібридним загрозам в інформаційному середовищі.

**Список використаних джерел:**

1. Thiele, R. (2021). *Hybrid Warfare*. Springer VS Wiesbaden.

230 p. https://doi.org/10.1007/978-3-658-35109-0

2. Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanit Soc Sci Commun*. 10, 360. https://doi.org/10.1057/s41599-023-01864-y

3. Merrin, W., Hoskins, A. (2024). Sharded War: seeing, not sharing. *Digi War*. https://doi.org/10.1057/s42984-023-00086-5

4. Where in Gaza is al-Ahli Arab Hospital, the site hit amid war with Israel? *Al Jazeera*. 18 October, 2023. URL: https://www.aljazeera.com/news/2023/10/18/where-in-gaza-is-al-ahli-arab-hospital-the-site-hit-amid-war-with-israel

**Сотник Анастасія**
*студентка географічного факультету*
*Київського національного університету імені Тараса Шевченка*

## НАСЛІДКИ ОКУПАЦІЇ АВТОНОМНОЇ РЕСПУБЛІКИ КРИМ

За словами Жан-Жака Елізе Реклю, історія – це географія в часі, а географія – це історія в просторі, відповідно хто не знає історію, тому виправляють географію, всіма можливими способами.

Крим – стратегічно важливий регіон для України та росії. Його історія та статус до анексії 2014 року були однією з передумов та причин конфлікту між росією та Україною зараз. Період з 2014 по 2024 роки прийнято вважати «гібридною фазою» хронології російсько-української війни.

Гібридні загрози – скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів, за використанням широкого кола засобів [1]. Основними їх цілями є безпосередньо суспільства-супротивники, а не бійці, оскільки, нівелювання відмінності між учасниками бойових дій та цивільним населенням веде до досягнення «результатів» без реальної війни.

Таке розмиття понять дозволяє, по-перше, створювати в державі штучну політичну кризу, яка уможливлює тимчасовий колапс комунікацій між центром та регіонами. Стану штучної кризи передує, з одного боку, відповідне медіа-аранжування та формування порядку денного державної нестабільності, сепаратистських рухів, некерованості в регіонах і т.п. У медіа-аранжуванні беруть участь агенти впливу зовнішніх центрів влади в органах державної влади та управління, культурні трендсеттери, громадські організації. По-друге, скористатися масовими безпорядками (групами «політичних активістів») для захоплення органів влади на місцях. При цьому

«політичні активісти» створюють димову завісу для дій недержавних збройних формувань, які беруть під контроль стратегічні об'єкти. На захопленій території відбувається мобілізація «народного ополчення» під релігійними гаслами, до чого підключається також і церква. По-третє, легітимізувати захоплення території шляхом проведення референдуму, обґрунтовуючи це потребою захисту етнічних меншин від громадянської війни. Зацікавлені у зовнішньому впливі сторони, при цьому, представляють діаметрально протилежні версії подій. Так, у розумінні ЄС та НАТО, події, що відбуваються, є звичайною війною, яка ведеться без публічного оголошення і з використанням ресурсу приватних армій та кримінальних угруповань, які виконують функції регулярних військових формувань. Але це, звісно, один бік медалі. Другим боком є те, що мас-медіа під дією проросійського впливу подає події в Україні як проєкт неоокупації та неоколоніалізму із використанням політичного комісаріату, технологій кольорових революцій та державного перевороту (в термінології російської пропаганди йдеться про «маріонеткову хунту військових злочинців») [2, с. 18].

Розглядаючи анексію з точки зору міжнародного права, безперечно, її статус досить очевидний. Окрім банального порушення територіальної цілісності суверенної України, росія порушила підписаний за її же участю у 1994 році загальновідомий Будапештський меморандум, за яким вона брала на себе зобов'язання гарантувати територіальну цілісність української держави, поважати її незалежність, суверенітет та існуючі кордони. Вочевидь, усі дії країни-агресора за останні роки, починаючи з загрози та використання сили проти політичної незалежності України, а саме, гібридної війни на сході з підтримкою сепаратистських рухів всередині країни, не кажучи вже про згадані порушення прав людини у контексті русифікації та репресій проти кримських татар, не можуть бути ратифіковані будь-якою країною цивілізованого світу, окрім, очевидно, тоталітарних проксі-країн по типу Білорусі або КНДР. Загалом, лише після 18 березня 2014 року у результаті прийняття так званого «Договору між російською федерацією і Республікою Крим про прийняття в російську федерацію Республіки Крим і утворення в складі російської федерації нових 'суб'єктів'»

росія порушила:

1. Міжнародно-правові принципи: а) територіальної цілісності держав; б) недоторканності державних кордонів; в) рівності та самовизначення народів; г) вирішення міжнародних спорів мирним шляхом; ґ) міжнародного співробітництва; д) суверенної рівності держав.

2. Всі дво- та багатосторонні міжнародні договори, згідно з якими РФ визнавала територіальну цілісність України, недоторканність українсько-російського кордону, а також територіальну приналежність Кримського півострова Україні.

3. Положення Женевських конвенцій 1949 р., оскільки РФ, внаслідок укладення Договору про Крим, юридично змінювала де-факто окупацію Кримського півострова на режим національної території, на який вимоги Женевських конвенцій об'єктивно не можуть розповсюджуватися.

4. Фундаментальні положення Конституції РФ, які становлять основи конституційного ладу РФ [4].

Отже, укладення РФ Договору про Крим є кульмінацією російської агресії на території Кримського півострова, яка завдала набагато більше шкоди міжнародному правопорядку, ніж будь-які порушення чи зловживання міжнародним правом з боку інших держав у XXI столітті.

Абсолютна більшість країн світу засуджує агресивні дії росії щодо України, накладає на країну-агресора санкції. Анексія широко засуджується на дипломатичному полі багатьма державами у вигляді осуду на міжнародних форумах та різних заходах, таких як спільні заяви, резолюції та рішення.

Переважна більшість цивілізованого світу ввела економічні санкції проти росії за її незаконні дії. Ці санкції включають обмеження або повне припинення співпраці в економічній сфері, заборону на експорт та імпорт низки товарів та поступове витіснення росії з енергетичних ринків [3, с. 122].

Наслідки незаконної окупації півострова переслідують росію й у контексті політичної ізоляції – в результаті цього росія була виключена з міжнародного клубу країн великої вісімки, відомої як «G8».

16 січня 2017 року Україна звернулася до Міжнародного суду ООН із позовом проти російської федерації, пославшись на порушення росією двох конвенцій: Міжнародної конвенції про боротьбу з фінансуванням тероризму та Міжнародної конвенції про ліквідацію всіх форм расової дискримінації. Відповідне рішення суду ООН було оголошено 31 січня 2024 року, в ході котрого він встановив численні порушення росією обох конвенцій [5].

Отож, окупація росією Криму мала значний вплив, як складова частина агресивної політики проти України, а також визначила необхідність консолідації міжнародної спільноти та підтримки української територіальної цілісності.

**Список використаних джерел:**

1. Гібридні загрози – WARN. URL: https://warn-erasmus.eu/ua/glossary/gibridni-zagrozi/.

2. Гугнін Е.А. Гібридна війна як технологія зовнішнього впливу (на прикладі анексії Криму). Гарабітус, 2020. Вип. 20. С. 13-19.

3. Капітоненко М., Куса І., Талімончук А. Санкції проти росії: нинішній стан, перспективи, успіхи та прогалини багатостороннього міжнародного санаційного режиму, проти російської федерації. Київ: Міжнародний центр перспективних досліджень, 2019. 48 с.

4. Марусяк О.В. Анексія Криму російською федерацією як злочин агресії проти України: міжнародно-правові аспекти: Монографія. Чернівці: «Місто», 2016. С. 121-122.

5. Суд ООН у Гаазі виніс рішення за позовом України проти росії. Частково воно на користь Києва – BBC News Україна. BBC News Україна. URL: https://www.bbc.com/ukrainian/articles/cv2812l75v8o.

Науково-популярне електронне видання

# ЗБІРНИК ТЕЗ ДОПОВІДЕЙ ВСЕУКРАЇНСЬКОЇ СТУДЕНТСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «ГІБРИДНІ ВІЙНИ СУЧАСНОСТІ: СТІЙКІСТЬ ТА ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ»

**(28 березня 2024 року)**



Конференція відбулась в рамках проєкту
«Академічна протидія гібридним загрозам – WARN».

---

Гарн. Times New Roman. Обл.-вид. арк. 20,1.

---

Тексти опубліковано в авторському редагуванні.
Виготовлення макету і технічне редагування:
*Дмитро Стретович*

---

Національний університет «Острозька академія»
Україна, 35800, Рівненська обл., м. Острог, вул. Семінарська, 2