12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 25.03.2026).
13. OECD. Regional Development Policy in Ukraine: Supporting Recovery and Resilience. Paris : OECD Publishing, 2023. URL: https://www.oecd.org (дата звернення: 25.03.2026).
14. European Commission. Ukraine Recovery and Reconstruction Plan. Brussels, 2022. URL: https://ec.europa.eu (дата звернення: 25.03.2026).
15. World Bank. Ukraine Rapid Damage and Needs Assessment (RDNA3). 2023. URL: https://www.worldbank.org (дата звернення: 25.03.2026).
UNDP. Ukraine Recovery and Resilience Framework. 2023. URL: https://www.undp.org (дата звернення: 25.03.2026).

Журавель Тетяна Олександрівна,
здобувачка другого (магістерського) рівня вищої освіти
спеціальності D4 «Публічне управління та адміністрування»
Миколаївський національний аграрний університет
Фізична особа-підприємець, власниця бізнесу
м. Миколаїв
ORCID : 0009-0006-2432-1142

ТРАНСКОРДОННЕ СПІВРОБІТНИЦТВО УКРАЇНИ ТА ЄС У СФЕРІ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Реформування теперішньої системи захищеності в Європі вирізняється переходом від класичних військових протистоянь до різнопланових гібридних протистоянь. Повномасштабне вторгнення рф в Україну дало зрозуміти, що межі фронту не завершуються лінією бойових дій. Гібридні загрози переносяться у транскордонний вимір, цим самим утворюють виклики для національної безпеки не лише України, а й сусідніх країн, які є державами-членами ЄС, наприклад Польщі, Словаччини, Румунії та Угорщини. Транскордонна зона, за своєю основою будучи відкритою системою з динамічним рухом капіталу, товарів та людських ресурсів, стає ідеальним опорним пунктом для застосування не силових засобів впливу – від масштабних кібератак на митну інфраструктуру до штучно інспірованих міграційних криз та масових інформаційно-психологічних операцій (ІПСО). У цьому розумінні звичні методи державного адміністрування кордонів виявляються недостатніми, що викликає важливу потребу в розробці сучасних механізмів транскордонного співробітництва, які б базувалися на принципах колективної стійкості та сумісних безпекових систем. Гібридна війна довела: безпека Варшави чи Братислави починається з інформаційної та кібернетичної стійкості Миколаєва, Харкова чи Києва. Це нова парадигма публічного управління, де захист спільних цінностей стає вищим за бюрократичні протоколи. Питання боротьби з гібридними загрозами та розвитку транскордонного співробітництва знаходяться у центрі уваги багатьох наших та зарубіжних науковців. Активна зміна методів гібридних впливів у 2024–2026

роках потребує переосмислення існуючих підходів та більше детального аналізу практичного досвіду взаємодії України з інституціями ЄС (Frontex, StratCom) в умовах затяжного конфлікту.

Метою дослідження є здійснення сукупного та структурованого аналізу існуючих і перспективних у розвитку механізмів транскордонного співробітництва між Україною та державами-членами ЄС, націлених на нейтралізацію багатопланових гібридних загроз національній безпеці. Мета передбачає не лише теоретичне усвідомлення явища гібридності в прикордонному просторі, а й формулювання прикладних, стратегічно орієнтованих рекомендацій щодо покращення системи державного адміністрування, збільшення її гнучкості та ефективності в умовах постійної безпекової нестабільності [6, с. 112]. Об'єктом дослідження є прогресивна сукупність суспільних відносин та процесів, що утворюються у межах транскордонної співпраці України з країнами Європейського співтовариства, а також кооперації інституційних сторін, уповноважених за формування та втілення безпекової політики у спільному європейському просторі.

Гібридні загрози подібні до вірусу: вони шукають не сильні сторони держави, а її вразливості – корупцію, соціальні розколи, недосконаліть законодавства. Тому протидія їм у межах транскордонного співробітництва не може бути суто військовою. Це має бути «інституційна дифузія» – процес, за якого органи управління України та ЄС настільки щільно обмінюються досвідом та даними, що будь-яка зовнішня дезінформація або кібератака блокується на рівні «імунітету» самої системи, ще до моменту завдання шкоди [3, с.45]. Транскордонний простір між Україною та державами-членами ЄС (зокрема Польщею, Словаччиною та Угорщиною) сьогодні функціонує не лише як зона економічної інтеграції, а як важливий елемент національної безпеки. Важлива риса гібридних небезпек полягає в їхній асиметричності та латентності, вони часто замасковані під дозволені соціальні протести, технічні збої або гуманітарні виклики. Для результативного державного адміністрування доречно класифікувати ці загрози за трьома стратегічними доменами:

Соціо-технічний домен: інструменталізація мобільності. Найбільш резонансним інструментом гібридного впливу є штучне управління міграційними потоками. На відміну від класичної міграції, гібридна модель передбачає:

- Створення контрольованого хаосу: використання великих груп людей для фізичного блокування пунктів пропуску, що паралізує роботу прикордонних та митних органів.

- Розмивання правового поля: свідоме порушення процедур перетину кордону з метою виснаження адміністративного ресурсу сил безпеки (Frontex, ДПСУ) [4, с. 94].

- Адміністративний виклик: потреба в миттєвому переході від сервісної моделі кордону до безпекової без зупинки стратегічних вантажопотоків.

Оскільки логістичні маршрути через західний кордон стали важливими для виживання української економіки, вони перетворилися на пріоритетні цілі: кібер-диверсії: DDoS-атаки на автоматизовані системи митного оформлення та

електронні черги, що призводять до багатокілометрових заторів; втручання в критичні системи: спроби дестабілізації енергомереж та залізничного управління в транскордонних хабах. Все це призводить до економічних збитків та затримка постачання товарів подвійного призначення, що прямо впливає на обороноздатність.

Когнітивно-інформаційний домен: дискредитація транскордонного партнерства. Ці загрози спрямовані на ментальний розрив між Україною та її найближчими союзниками [5, с. 142].. Основні напрями впливу:

1. Маніпуляція «аграрним питанням»: Вигадане роздування конфліктів навколо експорту зерна з метою дискредитації українських виробників в очах фермерів Польщі та Словаччини.

2. ІПСО на локальному рівні: Поширення через соціальні мережі фейків про «небезпечну поведінку» біженців або «корупцію на кордоні», що провокує негативний настрої серед місцевого населення прикордонних воєводств та областей.

3. Концептуальна війна: Використання болючих історичних тем для блокування міждержавного діалогу.

З цього всього ми можемо зробити висновки що, гібридні небезпеки у транскордонному просторі мають комплексний характер, де цифрова атака може бути синхронізована з міграційним тиском та інформаційною кампанією. Це вимагає від органів державного управління переходу до моделі інтегрованої безпеки, де координація відбувається не лише на рівні міністерств, а й на рівні оперативних штабів країн-сусідів.

Центральною фігурою в теорії публічного управління завжди була людина, але в умовах гібридності вона стає і головною мішенню, і головним елементом захисту. Транскордонне співробітництво має змістити фокус із «управління територіями» на «управління стійкістю громад». Коли мешканець прикордонного регіону здатен критично оцінити фейкову новину або захистити власні цифрові дані – це і є найвищою формою реалізації державної стратегії безпеки. Публічне управління має стати не наглядачем, а модератором, який надає громадянину інструменти для самозахисту в глобальному інформаційному просторі [2, с. 145]. Дієва протидія гібридним загрозам потребує відходу від лінійного управління до мережевої моделі взаємодії. Адміністрування в цій сфері має базуватися на принципах сумісності українських та європейських безпекових протоколів.

Стратегія Integrated Border Management (IBM), що впроваджується в межах співпраці з ЄС, є фундаментом для усунення гібридних ризиків.

Спільний контроль: впровадження пунктів спільного контролю (наприклад, на кордоні з Польщею) дозволяє зменшити час оформлення вантажів, що автоматично знижує ефективність гібридних атак, спрямованих на створення логістичних заторів.

Аналіз ризиків CIRAM: використання Спільної інтегрованої моделі аналізу ризиків (Common Integrated Risk Analysis Model), яку застосовує агентство Frontex. Це дозволяє розпізнати загрози (наприклад, аномальні міграційні рухи) ще до їхнього наближення до фізичного кордону.

*Адміністрування сучасного кордону неможливе без «цифрового щита». Ключовими напрямками є: з*ахист системи «Шлях» та митних баз даних: Створення дзеркальних серверів та впровадження хмарних технологій захисту, що майже унеможливлює параліч логістики через DDoS-атаки [1, с. 82]. Впровадження ШІ для моніторингу: Використання штучного інтелекту для аналізу відеопотоків та тепловізійних даних на «зеленому» кордоні, що дозволяє виявляти малопомітні диверсійні групи в автоматичному режимі.

Оскільки гібридна війна ведеться за розум та емоції, адміністративні заходи мають включати інформаційний складник:

Спільні пресцентри: Створення міждержавних комунікаційних хабів (Україна-Польща, Україна-Словаччина) для оперативного спростування фейків щодо аграрного експорту чи поведінки біженців.

Механізм раннього попередження (Early Warning System): Автоматизований обмін даними про виявлені ІПСО між Центром протидії дезінформації при РНБО та відповідними структурами ЄС (наприклад, East StratCom Task Force).

Майбутнє транскордонної взаємодії України та ЄС полягає у переході від моделі «ліквідації наслідків» до моделі «*превентивного адміністрування*». Гібридні загрози еволюціонують швидше за державні інституції. Тому створення спільних аналітичних хабів, де науковці та управлінці з України, Польщі та Словаччини зможуть моделювати загрози майбутнього (від кліматичного шантажу до ШІ-керованої дезінформації), є не просто бажаним, а життєво необхідним кроком для виживання європейського демократичного проєкту.

Під час проведеного нами дослідження теоретичних та прикладних аспектів транскордонного співробітництва України та ЄС в умовах гібридної війни, було сформульовано наступні положення і висновки:

Доведено, що транскордонний простір перестав бути лише зоною економічного обміну, перетворившись на об’єкт системних гібридних атак (кібердиверсій, інструменталізації міграції та дезінформаційних кампаній). Це вимагає від органів державного управління переходу від місцевого реагування до стратегічного адміністрування безпекових ризиків у синергії з європейськими інституціями. Найбільш ефективним інструментом протидії гібридним загрозам визначено модель інтегрованого управління кордонами, яка базується на спільних пунктах контролю та єдиних інформаційних базах даних (Eurosur, CIRAM). Це дозволяє мінімізувати часові витрати на логістику та унеможливлює використання «штучних черг» як інструменту економічного тиску.

Встановлено, що ключовим елементом адміністративного захисту є повна цифровізація митних та прикордонних процесів. Впровадження систем на основі штучного інтелекту для аналізу відеопотоків та захист критичних баз даних (система «Шлях», NCTS) дозволяє створити цифровий імунітет проти гібридних атак на інфраструктуру. Обґрунтовано необхідність створення транскордонних центрів стратегічних комунікацій (StratCom) на регіональному рівні (зокрема, для, Львівської областей та сусідніх воєводств Польщі та Словаччини). Це дозволить нейтралізувати спроби розпалювання соціальної ворожнечі в прикордонних громадах ще на етапі виникнення фейкових інфоприводів.

Практичне значення отриманих результатів полягає у можливості їх використання для вдосконалення Стратегії національної безпеки України в частині транскордонної взаємодії. Подальші дослідження мають бути спрямовані на розробку спільних з ЄС протоколів реагування на кібер-фізичні загрози в умовах глобальної цифровізації митного простору.

Список використаних джерел

1. Горбулін В. П. Як перемогти Росію у війні майбутнього. Київ : Брайт Букс, 2024. 256 с.

2.Дубов Д. В. Стратегічні комунікації в умовах гібридного протистояння : монографія. Київ : НІСД, 2022. 240 с.

3.Ковальова О. О. Протидія гібридним загрозам у транскордонному вимірі: виклики для України та ЄС : монографія. Київ : НІСД, 2025. 142 с.

4. Лукас Е. Спін-диктатори: як змінюється обличчя тиранії у XXI столітті. Київ Лабораторія, 2024. 320 с.

5. Почепцов Г. Г. Когнітивні війни в епоху цифровізації : монографія. Київ : Видавничий дім «Києво-Могилянська академія», 2025. 280 с.

6. Снайдер Т. Шлях до несвободи: Росія, Європа, Америка. 2-ге вид., допов. (2024–2026). Київ : Човен, 2025. 416 с.

Колесник Олександр Володимирович,
викладач вищої категорії,
викладач – методист Вінницький фаховий
коледж економіки і підприємництва Західноукраїнського
національного університету,
циклова комісія правових та психологічних дисциплін,
м. Вінниця, Україна
https://orcid.org/0000-0002-6995-983X
Кісіль Артем Андрійович,
здобувач передвищої освіти
спеціальності «Право»
Державний заклад: Віницького фахового коледжа
економіки та підприємництва
Західноукраїнського національного університета
м. Вінниця, Україна

КОМУНІКАТИВНА ПОЛІТИКА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ

У сучасних умовах розвитку України комунікативна політика органів місцевого самоврядування відіграє дуже важливу роль для ефективного управління на місцевому рівні. Вона охоплює всі форми взаємодії між владою та громадянами, а також допомагає формувати довіру до влади. Без налагодженої комунікації важко уявити демократичне суспільство, адже взаємодія з людьми є важливою умовою [3, с. 46] ефективної роботи місцевого самоврядування. Це означає, що громадяни мають не просто отримувати інформацію, а й мати змогу брати участь у прийнятті рішень. Наприклад, люди можуть подавати свої