МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ У СФЕРІ ОСВІТИ: ЗАХИСТ ВІД КОГНІТИВНИХ МАНІПУЛЯЦІЙ ТА ІНФОРМАЦІЙНИХ ВПЛИВІВ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Анатолій МАКАГОН

Науковий керівник роботи:
доктор юридичних наук, професор
_____ Лариса ВЕЛИЧКО

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. В умовах гібридної війни освітня сфера стала одним із ключових полів битви за свідомість громадян, де когнітивні маніпуляції та інформаційні впливи здатні підривати довіру до державних інститутів, деморалізувати молодь та впливати на формування національної ідентичності майбутніх поколінь. Освіта як соціальна система, що формує критичне мислення, ціннісні орієнтири та світогляд учнів і студентів, потребує особливого захисту від деструктивних інформаційних впливів, оскільки наслідки успішних когнітивних маніпуляцій у цій сфері мають довгостроковий характер і впливають на майбутнє держави.

Україна з 2014 року перебуває під систематичним інформаційним тиском Російської Федерації, спрямованим на дестабілізацію суспільства та підрив довіри до державних інституцій, а повномасштабне вторгнення 24 лютого 2022 року супроводжувалося інтенсифікацією дезінформаційних кампаній, що особливо активно таргетували освітню сферу через поширення фейків про безпеку шкіл, маніпуляції з історичною пам’яттю та атаки на систему дистанційного навчання. Прикордонні регіони, зокрема Харківська область, опинилися на передовій не лише збройного, а й інформаційного протистояння, де освітні заклади функціонують в умовах постійних обстрілів, психологічного тиску на педагогів і батьків та масштабних кампаній дезінформації про безпеку дітей у підземних школах і дистанційному навчанні.

Слід зазначити, що наявна система протидії інформаційним загрозам в освітній сфері формувалася реактивно, без достатньої координації між органами управління освітою, правоохоронними структурами та громадськими організаціями. Відсутність спеціалізованих підрозділів з моніторингу інформаційних загроз в освіті, недостатня підготовка педагогічних кадрів з медіаграмотності, обмежені технологічні можливості для виявлення дезінформації та хронічна нестача ресурсів створюють критичні вразливості для

когнітивних маніпуляцій, особливо в умовах масового переходу на дистанційне навчання та психологічного виснаження освітньої спільноти від життя під постійною загрозою.

Актуальність даного дослідження обумовлена нагальною потребою узагальнення унікального досвіду функціонування освітньої системи прикордонного регіону в умовах активних бойових дій, виявлення системних вразливостей до інформаційних впливів та розробки науково обґрунтованих практичних рекомендацій щодо вдосконалення механізмів публічного управління протидією гібридним загрозам в освіті.

Ефективна система захисту освітнього простору від когнітивних маніпуляцій є необхідною умовою не лише для збереження психологічної стійкості учнів та педагогів у воєнний час, але й для довгострокового забезпечення національної безпеки через формування покоління з критичним мисленням, здатного протистояти будь-яким формам інформаційних маніпуляцій у післявоєнний період.

Стан наукової розробки проблеми. Проблематика гібридних загроз та протидії інформаційним впливам перебуває у фокусі наукової уваги багатьох українських та зарубіжних дослідників, однак комплексні дослідження механізмів публічного управління протидією когнітивним маніпуляціям саме в освітній сфері прикордонних регіонів України досі залишаються фрагментарними.

Розглядаючи концептуальні засади гібридних загроз в освіті, Ю. Діма визначає гібридну війну як комплекс дій, де когнітивний вплив на освітню спільноту здійснюється через соціальні мережі, месенджери та маніпулятивний освітній контент. В. Сілайов аналізує політику інформаційної безпеки в умовах гібридних загроз та пропонує шляхи інституційного забезпечення протидії дезінформації на рівні публічного управління. С. Максименко, І. Деркач та О. Ірхін досліджують теоретико-психологічні детермінанти когнітивних маніпуляцій у воєнний час, виявляючи психологічні механізми вразливості населення прикордонних регіонів до інформаційних впливів.

Серед досліджень інформаційної безпеки в освіті слід звернути увагу на роботи О. Семененко, який аналізує воєнно-економічні дослідження когнітивного впливу на безпекову систему України, та Х. Германюк, яка вивчає публічне управління та адміністрування в умовах кібербезпеки.

Консорціум WARN у своїх дослідженнях узагальнює європейський досвід академічної протидії гібридним загрозам та адаптує його до українських реалій. Матеріали міжнародного конгресу з публічного управління XXI століття, організованого ННІ «Інститутом державного управління» Харківського національного університету імені В.Н. Каразіна, розкривають специфіку функціонування системи управління в умовах гібридних загроз на регіональному рівні.

О. Твердохліб аналізує освіту як соціальну систему у публічному управлінні національною безпекою, обґрунтовуючи критичну роль освітньої сфери для стратегічної стійкості держави. Д. Карамишев досліджує гібридні загрози і публічне управління з позицій теорії та практики, систематизуючи підходи до протидії. М. Погромський розглядає національну безпеку України в умовах гібридних загроз, виділяючи освітню складову як критичний елемент захисту. В. Гулай аналізує проблеми формування дефініції інформаційної безпеки у державному управлінні, що є важливим для понятійної визначеності досліджень у цій сфері. Г. Крохмаль досліджує трансформацію механізмів публічного управління у сфері безпеки освіти в умовах війни.

Серед зарубіжних науковців, які впливають на розуміння протидії гібридним загрозам в освіті, особливої уваги заслуговує досвід країн Балтії. Естонські дослідники систематизували практики захисту освітнього простору від російського інформаційного впливу після кібератак 2007 року, розробивши комплексну модель інтеграції кібербезпеки в національну освітню стратегію. Латвійські науковці зосереджуються на протидії історичному ревізіонізму через освітні програми, що є релевантним для українського контексту деколонізації освітнього простору. Литовські дослідники обґрунтували концепцію «активної стійкості» освітньої спільноти до інформаційних загроз через формування

молодіжних груп «інформаційних захисників» та інтеграцію медіаграмотності в усі рівні освіти.

Загалом, аналіз наукової літератури показує, що українські дослідники зосереджуються переважно на загальних концептуальних засадах гібридних загроз та правових аспектах інформаційної безпеки, тоді як зарубіжні науковці приділяють більшу увагу практичним механізмам формування медіаграмотності, технологічним інструментам моніторингу дезінформації та психологічним аспектам стійкості до когнітивних маніпуляцій.

Незважаючи на значну кількість досліджень окремих аспектів проблематики, відсутні комплексні роботи, які б системно аналізували механізми публічного управління протидією гібридним загрозам саме в освітній сфері прикордонних регіонів України в умовах активних бойових дій. Практично відсутні дослідження, які узагальнюють досвід функціонування освітньої системи Харківської області під постійними обстрілами, аналізують феномен підземних шкіл як інноваційну відповідь на виклики фізичної та інформаційної безпеки, та пропонують науково обґрунтовані практичні рекомендації, адаптовані до специфіки прикордонного регіону. Саме заповнення цієї прогалини визначає актуальність і практичну значущість даного дослідження.

Метою роботи є комплексний аналіз механізмів протидії гібридним загрозам у сфері освіти прикордонного регіону в умовах активних бойових дій та розробка науково обґрунтованих практичних рекомендацій для системи публічного управління освітою Харківської області щодо захисту від когнітивних маніпуляцій та інформаційних впливів.

Для досягнення поставленої мети визначено наступні *завдання:*

– узагальнити теоретико-методологічні засади протидії гібридним загрозам у сфері освіти та розробити типологію загроз для прикордонних регіонів;

– дослідити міжнародний досвід протидії інформаційним впливам в освіті шляхом компаративного аналізу практик країн-членів НАТО, зокрема країн Балтії, Фінляндії, Польщі та США;

– проаналізувати вітчизняний досвід протидії інформаційним загрозам в освіті через критичне дослідження ініціатив Міністерства освіти і науки України та регіональних практик;

– здійснити комплексний аналіз сучасного стану та вразливостей освітньої системи Харківської області до гібридних загроз, включаючи характеристику освітньої мережі, виявлення каналів інформаційного впливу та оцінку діяльності Департаменту науки і освіти ХОВА;

– виявити ключові виклики функціонування освітніх закладів Харківської області в умовах постійних обстрілів, психологічного тиску та інформаційних атак;

– розробити багаторівневий комплекс практичних рекомендацій для системи публічного управління освітою Харківської області, що включає інституційні, технологічні, освітні, психологічні та соціальні компоненти протидії гібридним загрозам.

Об'єктом дослідження є система протидії гібридним загрозам в освітній сфері України.

Предметом дослідження є механізми публічного управління протидією когнітивним маніпуляціям та інформаційним впливам в освітній системі Харківської області в умовах активних бойових дій.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів, застосування яких здійснювалося відповідно до специфіки кожного етапу дослідження.

Метод термінологічного аналізу застосовано для розмежування понять «гібридна загроза», «когнітивна маніпуляція», «інформаційний вплив», «дезінформація», що дозволило створити чітку термінологічну основу для аналізу феномену інформаційних загроз в освітній сфері (підрозділ 1.1). *Метод системного аналізу* використано для дослідження освітньої системи Харківської області як складної багаторівневої структури, що функціонує в умовах постійних зовнішніх загроз, виявлення взаємозв'язків між різними компонентами системи

та їхнього впливу на вразливість до інформаційних атак (підрозділ 3.1). *Компаративний аналіз* застосовано для порівняння практик протидії інформаційним загрозам в освіті країн-членів НАТО з вітчизняним досвідом, що дозволило ідентифікувати кращі практики для адаптації до українського контексту (розділ 2).

Інституційний аналіз використано для дослідження структури, повноважень та взаємодії органів публічного управління освітою Харківської області у протидії інформаційним загрозам, що виявило критичні прогалини в інституційній спроможності та координації між різними відомствами (підрозділ 3.1). *Структурно-функціональний аналіз* застосовано для визначення ролей та функцій Департаменту науки і освіти ХОВА, освітніх закладів, правоохоронних органів та громадських організацій у системі протидії гібридним загрозам, що допомогло ідентифікувати проблеми дублювання та координації (підрозділи 3.1, 3.2). *Нормативно-правовий аналіз* використано для вивчення регіональної нормативної бази протидії інформаційним загрозам в освіті, виявлення прогалин у правовому регулюванні на рівні Харківської області (підрозділ 3.1).

Метод документального аналізу застосовано для вивчення офіційних документів, планів роботи, розпоряджень Харківської обласної військової адміністрації, звітів про організацію освітнього процесу в умовах воєнного стану (підрозділ 3.1). *Метод контент-аналізу* використано для систематичного аналізу дезінформаційних наративів про освітні заклади Харківської області в соціальних мережах та месенджерах, виявлення типових шаблонів інформаційних атак та ефективності існуючих практик спростування (підрозділ 3.1). *Метод моніторингу* застосовано для відстеження та аналізу інформаційних інцидентів в освітній сфері Харківської області протягом 2023-2025 років (підрозділ 3.1).

Метод опитування використано для збору первинної інформації про рівень медіаграмотності педагогів та учнів Харківської області, їхній досвід зіткнення з дезінформацією та психологічний стан в умовах постійної

загрози (підрозділ 3.1). *Проблемно-орієнтований аналіз* застосовано для виявлення та систематизації ключових викликів і вразливостей освітньої системи Харківської області до інформаційних впливів (підрозділ 3.1). *Метод стратегічного планування* застосовано для визначення пріоритетних напрямів розвитку системи протидії гібридним загрозам в освіті Харківської області з урахуванням обмежених ресурсів воєнного часу, специфіки прикордонного регіону та критичності захисту освітнього простору (підрозділ 3.2). *Метод моделювання* використано для розробки комплексної моделі багаторівневої системи протидії інформаційним загрозам (підрозділ 3.2). *Метод пілотного проєктування* використано для розробки механізму поетапного впровадження рекомендацій через тестування в обмеженій кількості освітніх закладів з подальшим масштабуванням успішних практик (підрозділ 3.2).

Комплексне застосування зазначених методів дозволило забезпечити всебічність та об’єктивність дослідження механізмів протидії гібридним загрозам в освітній системі Харківської області.

Практичне значення отриманих результатів. Результати дослідження мають конкретне практичне застосування у декількох ключових сферах:

У науково-дослідній сфері матеріали роботи слугують для подальших наукових досліджень механізмів публічного управління протидією інформаційним загрозам в освіті прикордонних регіонів. Узагальнений досвід функціонування освітньої системи Харківської області в умовах постійних обстрілів та інформаційних атак становить унікальний матеріал для наукового аналізу стійкості соціальних систем у екстремальних умовах та збагачує академічну дискусію про освіту в умовах війни.

Феномен підземних шкіл Харкова, вперше комплексно проаналізований у контексті вразливостей до інформаційних загроз, формує нову дослідницьку область на перетині архітектури безпеки, педагогіки стресу та інформаційної війни.

У практичній діяльності регіональних органів влади результати дослідження надають Харківській обласній військовій адміністрації аналітичну

основу при розробці та вдосконаленні регіональних стратегічних документів з питань інформаційної безпеки освіти та протидії когнітивним маніпуляціям.

Департамент науки і освіти Харківської ОВА отримує конкретні практичні рекомендації щодо створення спеціалізованих структур з моніторингу інформаційних загроз, координації з правоохоронними органами та впровадження технологічних рішень для захисту освітнього простору, які враховують реальні можливості та обмеження регіональних органів у воєнний час. Освітні заклади Харківської області можуть застосовувати результати дослідження при розробці локальних планів протидії дезінформації, організації тренінгів з медіаграмотності для педагогів та учнів, створенні систем швидкого реагування на фейкові повідомлення про безпеку.

Запропонований комплекс рекомендацій з розрахунком бюджетів та індикаторами ефективності формує основу середньострокових планів розбудови системи захисту освітнього простору Харківської області від інформаційних впливів.

Узагальнені практики створення підземних навчальних просторів, організації дистанційного навчання в умовах нестабільного інтернету та психологічної підтримки освітньої спільноти під постійною загрозою можуть бути використані іншими прикордонними регіонами України (Сумська, Чернігівська, Донецька області) для адаптації досвіду Харкова до локальних умов. Аналіз ефективності різних каналів комунікації між адміністрацією, педагогами та батьками в умовах інформаційних атак забезпечує практичні орієнтири для оптимізації комунікаційних стратегій освітніх закладів.

У практичній діяльності центральних органів влади Міністерство освіти і науки України отримує критичний аналіз ефективності власних ініціатив у сфері інформаційної безпеки освіти з конкретними рекомендаціями щодо вдосконалення національної стратегії, зокрема необхідності створення системної програми медіаграмотності, забезпечення технологічного захисту освітніх платформ та інтеграції психологічної стійкості до когнітивних маніпуляцій у програми підтримки.

Служба безпеки України та Національна поліція можуть застосовувати виявлені шаблони дезінформаційних кампаній для швидшого виявлення та блокування фейкових акаунтів і каналів, що таргетують освітню спільноту.

У навчальному процесі матеріали дослідження можуть бути інтегровані закладами вищої освіти при викладанні дисциплін «Публічне управління та адміністрування», «Інформаційна безпека», «Управління освітою в умовах кризи», « Публічне управління на деокупованих територіях» доповнюючи їх запропонованими актуальними кейсами з досвіду Харківської області.

Результати дослідження можуть бути включені до програм підготовки та підвищення кваліфікації керівників освітніх закладів, педагогічних працівників та публічних службовців у Національному агентстві України з питань державної служби, ННІ «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна, обласних інститутах післядипломної педагогічної освіти, зокрема для фахівців з питань інформаційної безпеки в освіті.

Матеріали роботи можуть бути використані при підготовці навчально-методичних посібників, монографій, наукових статей з проблематики протидії гібридним загрозам в освіті, при розробці нових освітньо-професійних програм магістрів публічного управління з спеціалізацією на управлінні освітою в умовах кризи, а також підготовки фахівців у сфері освітньої безпеки, стратегічних комунікацій в освіті та педагогіки в екстремальних умовах.

Апробація результатів дослідження. Основні положення та результати роботи обговорювалися на засіданнях кафедри права, національної безпеки та європейської інтеграції ННІ «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна і можуть бути використані в подальшому в науковій та викладацькій діяльності кафедри, зокрема при розробці нових навчальних курсів з управління освітою в умовах кризи та інформаційної безпеки в публічному секторі.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У СФЕРІ ОСВІТИ

1.1 Концептуальні основи гібридних загроз та когнітивних маніпуляцій в освітньому просторі

Гібридні загрози в освітній сфері являють собою комплекс синхронізованих впливів, що поєднують традиційні та нетрадиційні методи ведення війни з метою дестабілізації освітнього простору та маніпулювання свідомістю учасників освітнього процесу. У сучасному науковому дискурсі, зокрема В. Сілайовим, гібридна загроза визначається як багатовимірний феномен, що об’єднує військові, політичні, економічні, інформаційні та психологічні компоненти впливу [74]. Специфіка воєнного стану в Україні, зокрема в прикордонних регіонах, надає цим загрозам особливої інтенсивності та цілеспрямованості. За переконанням С. Максименко, І. Деркача та інших співавторів, когнітивні маніпуляції в період збройного конфлікту набувають системного характеру, впливаючи на базові механізми сприйняття та обробки інформації [35].

Когнітивні маніпуляції в освітньому контексті розуміються як цілеспрямовані дії, направлені на викривлення процесів мислення, сприйняття та прийняття рішень учасниками освітнього процесу через використання психологічних вразливостей та інформаційних технологій. О. Семененко розглядає когнітивний вплив як системну операцію, що спрямована на підрив критичного мислення та формування бажаних для агресора поведінкових патернів (зразків) [70].

Дійсно, в умовах воєнного стану ці маніпуляції часто маскуються під турботу про безпеку, використовуючи природну тривожність населення

прикордонних регіонів. Х. Германюк підкреслює, що в епоху цифрової трансформації когнітивні атаки набули нових форм, використовуючи можливості соціальних мереж та месенджерів для масштабного розповсюдження деструктивного контенту [12].

Інформаційний вплив в освітній сфері характеризується як комплекс заходів, спрямованих на зміну інформаційного середовища освітніх закладів з метою формування бажаних атитюдів, переконань та поведінкових моделей. Консорціум WARN у своєму дослідженні виділяє три основні форми інформаційного впливу: пряма пропаганда, латентна дезінформація та маніпулятивний контент, замаскований під освітні матеріали [30].

Матеріали XXII міжнародного конгресу з публічного управління свідчать, що в умовах гібридної війни інформаційний вплив часто здійснюється через, здавалося б, нейтральні канали комунікації [47]. Особливої уваги заслуговує феномен використання мемів та візуального контенту для когнітивного впливу, що на думку М. Давидюка, демонструє адаптацію пропагандистських методів до сучасної медіакультури молоді [17].

Дезінформація в освітньому просторі розуміється як навмисне поширення недостовірної або викривленої інформації з метою введення в оману учасників освітнього процесу та дестабілізації довіри до інституцій. Л. Войналович аналізує когнітивний вимір метафор у публічному дискурсі, демонструючи, як лінгвістичні конструкції використовуються для маніпулювання сприйняттям безпекової ситуації [8].

В умовах воєнного стану дезінформація часто стосується питань безпеки освітніх закладів, графіків навчання та евакуації. І. Семенець-Орлова підкреслює, що системна протидія дезінформації вимагає комплексного підходу з боку органів публічного управління [71]. Дослідження Є. Ніколаєва, Г. Рій та ін. показують, як війна трансформувала інформаційне середовище вищої освіти України, створюючи нові канали для розповсюдження неперевірених даних [46].

Для систематизації розглянутих вище понять та демонстрації їх взаємозв’язку в умовах воєнного стану доцільно представити основні категорії

понятійного апарату у структурованому вигляді.

Таблиця 1.1 – Основні категорії понятійного апарату протидії гібридним загрозам в освіті

Поняття	*Визначення*	*Специфіка в умовах воєнного стану*	*Канали реалізації*	*Об'єкти впливу*
Гібридна загроза	Комплекс синхронізованих військових, інформаційних, економічних та психологічних впливів	Посилення інтенсивності, використання страху та невизначеності	Соціальні мережі, месенджери, фейкові новини, координовані атаки	Учні, студенти, педагоги, батьки, адміністрація
Когнітивна маніпуляція	Цілеспрямоване викривлення процесів мислення та сприйняття	Експлуатація травми, тривожності та стресу населення	Емоційний контент, фейки про безпеку, псевдоекспертні думки	Критичне мислення, процеси прийняття рішень, довіра до інституцій
Інформаційний вплив	Заходи зі зміни інформаційного середовища для формування бажаних атитюдів	Використання воєнного контексту для легітимізації впливу	Telegram-канали, TikTok, замасковані освітні ресурси	Світогляд, ціннісні орієнтири, патріотична свідомість
Дезінформація	Навмисне поширення недостовірної інформації	Фейки про обстріли шкіл, евакуацію, графіки роботи	Анонімні повідомлення, ботоферми, маніпуляції зі скріншотами	Емоційний стан, відчуття безпеки, довіра до влади
Пропаганда	Систематичне розповсюдження ідеологічно забарвленого контенту	Антиукраїнські наративи, історичний ревізіонізм	Контент для молоді, ігрові платформи, навчальні матеріали	Національна ідентичність, історична пам'ять, мовна політика

Джерело: розробка автора на основі узагальнення наукових джерел [74, 35, 70, 12, 46].

Аналіз представленої таблиці 1.1 демонструє багатовимірність понятійного апарату та складність гібридних загроз в освітньому просторі прикордонних регіонів. Особливо важливим є розуміння того, що кожна категорія загроз має специфічні прояви в умовах воєнного стану, використовуючи психологічну вразливість населення, яке щодня перебуває під

загрозою обстрілів. Канали реалізації загроз є надзвичайно різноманітними, від традиційних соціальних мереж до новітніх платформ, популярних серед молоді.

Об’єкти впливу охоплюють усі групи учасників освітнього процесу, що вимагає комплексного підходу до протидії. Важливо зазначити, що гібридні загрозі діють не ізольовано, а в синергії, посилюючи один одного та створюючи кумулятивний ефект на освітнє середовище. Системне розуміння цих категорій є необхідною передумовою для розробки ефективних механізмів протидії та формування стійкості освітнього простору регіону до деструктивних впливів.

Типологізація гібридних загроз для прикордонних регіонів вимагає врахування специфічних умов їхнього функціонування, зокрема близькості до лінії фронту, історії окупації та постійної загрози ракетних обстрілів. Навчальна програма Erasmus+ WARN виділяє три основні кластери загроз для освітнього простору прикордонних територій: інформаційно-комунікативні, психологічні та безпекові [13].

Так, А. Семеренко підкреслює, що психологічна стійкість населення прикордонних регіонів є першочерговою мішенню гібридних операцій, оскільки її підрив автоматично послаблює всі інші компоненти національної безпеки [72]. В контексті Харківської області особливої актуальності набувають загрози, пов'язані з маніпулюванням відчуттям безпеки та створенням атмосфери невизначеності щодо можливості продовження освітнього процесу.

Інформаційні атаки на освітній простір прикордонних регіонів характеризуються високою інтенсивністю, координованістю та адаптивністю до локального контексту. Такі атаки включають:

а) масове розповсюдження фейків про обстріли освітніх закладів з метою посилення паніки та дезорганізації навчального процесу;

б) цільові кампанії дезінформації щодо безпеки конкретних шкіл або університетів для провокування евакуації та переривання навчання;

в) маніпуляції з візуальним контентом, включаючи підроблені фотографії та відео руйнувань освітніх об’єктів;

г) створення фейкових акаунтів адміністрації закладів освіти для

розповсюдження панічних повідомлень;

д) координовані атаки в соціальних мережах на керівництво освітніх закладів з метою підриву довіри до адміністрації.

Зокрема, О. Твердохліб розглядає освіту як соціальну систему, що потребує особливого захисту в умовах національної безпеки, підкреслюючи, що інформаційні атаки на освітній простір є стратегічним елементом гібридної війни [76], а В. Гулай аналізує складність формування дефініції інформаційної безпеки в контексті державного управління, що ускладнює координацію протидії загрозам [15].

Психологічний тиск на учасників освітнього процесу в прикордонних регіонах здійснюється через систематичне використання травмуючих образів, створення атмосфери безперервної загрози та експлуатацію природних батьківських страхів за безпеку дітей. В цьому аспекті, Г. Крохмаль досліджує трансформацію механізмів публічного управління у сфері безпеки освіти, зазначаючи, що психологічний вплив часто є більш руйнівним, ніж пряме фізичне знищення інфраструктури [34]. На думку науковця, психологічний тиск реалізується через декілька механізмів:

– постійне нагнітання страху через повідомлення про можливі атаки на школи;

– створення відчуття безпорадності шляхом підриву довіри до можливості органів влади забезпечити безпеку;

– формування негативного образу дистанційного навчання як неповноцінної форми освіти;

– провокування конфліктів між батьками, педагогами та адміністрацією навколо питань безпеки навчання.

М. Козир слушно підкреслює, що безпечне освітнє середовище в умовах війни вимагає не лише фізичного захисту, а й психологічної підтримки всіх учасників процесу [29].

Дезінформація про безпеку в освітніх закладах прикордонних регіонів становить окремий критичний виклик, оскільки безпосередньо впливає на

можливість продовження освітнього процесу та психологічний стан дітей і педагогів. Зокрема, І. Хоменко досліджує питання цифрової безпеки освітнього простору, зазначаючи, що дезінформація про загрози часто поширюється швидше за офіційні повідомлення [82]. На його думку, дезінформація про безпеку включає:

1) фальшиві тривожні повідомлення про ракетні атаки в години навчальних занять;

2) поширення неперевірених даних про руйнування конкретних шкіл для створення паніки;

3) маніпуляції з графіками роботи укриттів в освітніх закладах;

4) фейкові розпорядження про евакуацію учнів або закриття закладів;

5) псевдоекспертні коментарі про небезпечність відвідування шкіл у певних районах.

Цікавим вбачається дослідження О. Давиденко, який аналізує інформаційну стійкість навчальних закладів у критичних ситуаціях, підкреслюючи важливість швидкої верифікації інформації та наявності надійних каналів комунікації [16].

На основі аналізу наукових джерел та міжнародного досвіду протидії гібридним загрозам доцільно представити комплексну типологію загроз для освітнього простору прикордонних регіонів, що дозволить систематизувати різні форми їх прояву та визначити найбільш ефективні механізми протидії

Таблиця 1.2 – Типологія гібридних загроз для освітнього простору прикордонних регіонів

Тип загрози	*Форми прояву*	*Цільові групи*	*Очікувані наслідки*	*Індикатори загрози*	*Міжнародні аналоги*
Інформаційні атаки	Фейки про обстріли шкіл, маніпуляції з фото/відео, фальшиві акаунти адміністрації, координовані	Батьки, педагоги, локальна спільнота	Паніка, евакуація, перерви в навчанні, втрата довіри до влади	Різке зростання згадок про небезпеку в соцмережах, активність ботоферм, аномальна	Досвід країн Балтії з протидією інформаційним атакам РФ (2014-2024)

	тролінг-кампанії			поведінка акаунтів	

Продовження таблиці 1.2

Тип загрози	*Форми прояву*	*Цільові групи*	*Очікувані наслідки*	*Індикатори загрози*	*Міжнародні аналоги*
Психологічний тиск	Нагнітання страху, травмуючий візуальний контент, провокування конфліктів, підрив довіри до інституцій	Учні, студенти, батьки, вчителі	Хронічний стрес, травматизація, відмова від очного навчання, професійне вигорання педагогів	Зростання тривожності в опитуваннях, збільшення звернень до психологів, падіння відвідуваності	Фінський досвід психологічної підтримки в умовах гібридної загрози
Дезінформація про безпеку	Фальшиві повідомлення про атаки, маніпуляції з графіками роботи укриттів, псевдоекспертні коментарі	Вся освітня спільнота, органи управління	Дезорганізація процесу, непродумані рішення про евакуацію, втрата часу на перевірку фейків	Невідповідність інформації офіційним джерелам, швидкість поширення, емоційний окрас	Польський досвід верифікації інформації в прикордонних зонах
Когнітивні маніпуляції	Історичний ревізіонізм, мовні провокації, підміна понять, культурна експансія	Учні, молодь, студенти	Розмивання національної ідентичності, конфлікти на мовному ґрунті	Поява антиукраїнських наративів у молодіжному середовищі	Естонський досвід захисту національної ідентичності в освіті
Кібератаки на освітні системи	DDoS-атаки на освітні платформи, злам баз даних, розповсюдження шкідливого ПЗ	IT-інфраструктура, адміністратори, користувачі	Втрата даних, неможливість дистанційного навчання, витік персональних даних	Технічні збої, аномальна активність у системах, спроби несанкціонованого доступу	Литовський досвід кіберзахисту освітніх систем

Джерело: Розробка автора на основі узагальнення міжнародного досвіду та аналізу загроз [63, 26, 83, 13, 59].

Представлена типологія демонструє багатоплановість та взаємопов’язаність гібридних загроз для освітнього простору прикордонних регіонів, що вимагає комплексного та багаторівневого підходу до протидії. Аналіз міжнародних аналогів показує, що країни Балтії та Польща, які мають

тривалий досвід протистояння російським гібридним операціям, розробили ефективні механізми раннього виявлення та нейтралізації подібних загроз.

Особливо цінним є Естонський досвід створення національної системи кіберзахисту та фінська модель психологічної стійкості суспільства, що можуть бути адаптовані до українських реалій. Критично важливим є розуміння індикаторів загроз, що дозволяє органам управління освітою своєчасно реагувати на потенційні атаки. Очікувані наслідки кожного типу загроз підкреслюють необхідність превентивних заходів, оскільки ліквідація наслідків вимагає значно більших ресурсів, ніж попередження. Взаємозв'язок різних типів загроз створює ефект домінування, коли актуалізація однієї загрози автоматично збільшує вразливість до інших, що необхідно враховувати при розробці стратегій протидії.

В. Сілайов підкреслює важливість інституційної реакції державних органів на когнітивні впливи, зазначаючи, що швидкість та координованість відповіді значною мірою визначають масштаб наслідків гібридних атак [73]. О. Семененко аналізує інституційну готовність до кризових когнітивних атак, виявляючи критичні прогалини в системі протидії на регіональному рівні [69]. О. Косянчук досліджує специфіку цифрової освітньої безпеки в умовах війни, підкреслюючи необхідність інтеграції технологічних та гуманітарних підходів до захисту освітнього простору [31].

Критичний аналіз розглянутих вище наукових позицій і зарубіжних практик свідчить про визнання дослідниками багатовимірності гібридних загроз для освітнього простору. Водночас простежується фрагментарність підходів до протидії: різні автори акцентують увагу на технологічному (О. Косянчук, Хоменко), інституційному (Сілайов, О. Семененко) чи психологічному (Семеренко, Козир) аспектах, без достатньої інтеграції у єдину систему.

Особливо відчутною є потреба у розробці специфічних механізмів для прикордонних регіонів з урахуванням високої інтенсивності загроз та обмежених ресурсів. Міжнародний досвід країн Балтії та Фінляндії потребує критичної адаптації до українського контексту воєнного стану.

Підсумовуючи, понятійно-категоріальний апарат протидії гібридним загрозам в освіті формує теоретичну основу для розуміння механізмів інформаційного впливу в умовах воєнного стану. Специфіка прикордонних регіонів полягає в інтенсифікації всіх форм когнітивних маніпуляцій, що використовують психологічну вразливість населення та невизначеність безпекової ситуації для досягнення стратегічних цілей агресора.

Типологія гібридних загроз для прикордонних регіонів характеризується підвищеною інтенсивністю інформаційних атак, систематичним психологічним тиском та масштабною дезінформацією про безпеку освітніх закладів.

Міжнародний досвід країн Балтії та Фінляндії демонструє можливість ефективної протидії таким загрозам через створення комплексних систем моніторингу, швидкого реагування та психологічної підтримки освітньої спільноти.

1.2 Методологія дослідження протидії інформаційним впливам в регіональній системі освіти

Методологія дослідження ефективності механізмів публічного управління протидією інформаційним впливам в регіональній системі освіти базується на інтеграції кількісних та якісних методів, що дозволяє отримати комплексне уявлення про стан та динаміку процесів у цій сфері. Зокрема, О. Таран розглядає когнітивну стійкість як об’єкт публічного управління в освіті, пропонуючи системний підхід до оцінки ефективності управлінських рішень [75].

На нашу думку, в умовах кризи, спричиненої воєнним станом, традиційні методи дослідження потребують адаптації до специфіки прикордонних регіонів, де освітній процес відбувається в умовах постійної загрози. Так, Л. Іщенко підкреслює важливість механізмів підвищення цифрової грамотності педагогів як ключового елементу протидії дезінформації, що вимагає розробки

спеціальних інструментів моніторингу та оцінки [27].

Дійсно, кількісні методи дослідження повинні включати статистичний аналіз даних про інформаційні інциденти в освітніх закладах, частоту виявлення дезінформації, швидкість реагування органів управління на загрози та результати впровадження протидійних заходів. Матеріали міжнародної конференції «Людина і цифрове суспільство: когніція-мова-освіта-дискурс» демонструють важливість використання Big Data для виявлення шаблонів інформаційних атак та прогнозування потенційних загроз [24]. Основні кількісні показники включають:

а) частоту інформаційних інцидентів (кількість зафіксованих випадків дезінформації на тиждень/місяць);

б) час реагування органів управління на виявлені загрози (від моменту виявлення до початку контрзаходів);

в) охоплення освітньої спільноти програмами медіаграмотності (відсоток педагогів та учнів, що пройшли навчання);

г) рівень довіри до офіційних джерел інформації (за результатами регулярних опитувань);

д) ефективність верифікації повідомлень (відсоток швидко спростованих фейків до загальної кількості).

Дані дослідження підкреслюють необхідність використання адаптивних методологій, що враховують динамічні зміни в умовах кризи та дозволяють коригувати стратегії протидії в режимі реального часу і підтверджують нашу позицію.

Якісні методи дослідження спрямовані на глибинне розуміння механізмів впливу гібридних загроз, суб’єктивного сприйняття учасниками освітнього процесу безпекової ситуації та ефективності управлінських рішень. Зокрема, Л. Войцехівська досліджує психологічну грамотність учителів як чинник протидії маніпуляціям, що вимагає застосування глибинних інтерв’ю та фокус-груп для виявлення латентних проблем [9]. Якісні методи на думку дослідниці включають:

– напівструктуровані інтерв’ю з керівниками освітніх закладів, педагогами, батьками та учнями для з’ясування їхнього досвіду зіткнення з дезінформацією;

– фокус-групи з представниками освітньої спільноти для обговорення ефективності існуючих механізмів протидії;

– кейс-стаді успішних та неуспішних випадків реагування на інформаційні атаки;

– аналіз документів, включаючи розпорядчі акти органів управління освітою, протоколи нарад, звіти про інциденти;

– спостереження за функціонуванням системи комунікації в освітніх закладах під час кризових ситуацій.

В. Гулай слушно зазначає, що якісні методи дозволяють виявити приховані вразливості системи, які не фіксуються статистичними показниками [15] і тому вважаємо, що змішані методи дослідження, що поєднують кількісні та якісні підходи, забезпечують найбільш повне розуміння ефективності механізмів публічного управління в умовах кризи. О. Твердохліб підкреслює, що інтеграція різних методологій дозволяє триангулювати дані та підвищити достовірність висновків [76].

Тріангуляція даних з різних джерел (офіційна статистика, опитування, інтерв'ю, моніторинг соціальних мереж) дозволяє перевірити надійність інформації та виявити розбіжності між офіційними даними та реальною ситуацією. Лонгітюдний дизайн дослідження з регулярними вимірюваннями показників дає змогу відстежити динаміку змін та оцінити вплив впроваджених заходів протягом тривалого періоду.

Порівняльний аналіз між різними районами Харківської області виявляє локальні особливості та дозволяє виявити кращі практики для тиражування. Розробка критеріїв оцінки стійкості освітнього середовища до когнітивних маніпуляцій є ключовим методологічним завданням, що дозволяє об’єктивно вимірювати ефективність протидійних заходів та виявляти вразливі точки системи.

Так, Г. Крохмаль визначає стійкість освітнього середовища як інтегральну характеристику, що відображає здатність системи зберігати функціональність та цілісність під впливом деструктивних інформаційних операцій [34]. М. Козир підкреслює, що безпечне освітнє середовище в умовах гібридної війни передбачає не лише захист від зовнішніх загроз, а й внутрішню спроможність до самовідновлення та адаптації [29]. Розробка системи критеріїв має базуватися на міжнародному досвіді, зокрема фінській моделі суспільної стійкості та естонських стандартах інформаційної безпеки в освіті.

Інституційні критерії стійкості відображають спроможність органів управління освітою та освітніх закладів ефективно протидіяти інформаційним загрозам через наявність відповідних структур, процедур та ресурсів.

Підкреслюючи важливість інституційної спроможності для координації протидійних заходів, І. Хоменко провів дослідження цифрової безпеки освітнього простору [82]. На думку науковця, ключові інституційні критерії включають:

а) наявність спеціалізованих підрозділів з моніторингу та протидії інформаційним загрозам у структурі органів управління освітою;

б) розробленість нормативно-правової бази на регіональному рівні щодо інформаційної безпеки в освітніх закладах;

в) функціонування систем раннього попередження про потенційні інформаційні атаки та дезінформаційні компанії;

г) ефективність каналів комунікації між різними рівнями управління освітою для швидкого реагування;

д) наявність протоколів дій у випадку різних типів інформаційних інцидентів;

е) ресурсне забезпечення програм протидії дезінформації та розвитку медіаграмотності.

Аналізуючи інформаційну стійкість навчальних закладів у критичних ситуаціях, О. Давиденко зазначає, що інституційна спроможність є базовою передумовою для всіх інших форм стійкості [16].

Компетентнісні критерії стійкості характеризують рівень готовності учасників освітнього процесу розпізнавати та протистояти когнітивним маніпуляціям через наявність відповідних знань, умінь та навичок. В цьому аспекті, Л. Іщенко підкреслює, що механізми підвищення цифрової грамотності педагогів є критично важливими для формування стійкого освітнього середовища [27].

Л. Войцехівська досліджуючи психологічну грамотність учителів як ключовий захисний фактор проти маніпулятивних впливів [9] виділяє компетентнісні критерії, які на думку авторки охоплюють:

– рівень медіаграмотності педагогів (здатність критично оцінювати інформацію, верифікувати джерела, розпізнавати маніпулятивні техніки);

– навички цифрової гігієни учнів та студентів (обізнаність про безпечну поведінку в мережі, розуміння ризиків);

– здатність батьків підтримувати дітей у формуванні критичного мислення;

– компетентність адміністрації закладів у питаннях інформаційної безпеки;

– наявність навичок психологічної саморегуляції для протидії стресу від інформаційних атак.

Технологічні критерії стійкості відображають рівень захищеності цифрової інфраструктури освітніх закладів та ефективність використання технологічних рішень для протидії інформаційним загрозам. Так, О. Косянчук досліджує цифрову освітню безпеку в умовах війни, підкреслюючи необхідність інтеграції сучасних технологічних рішень [31], а матеріали міжнародної конференції з когніції та освіти демонструють важливість технологічної складової для забезпечення стійкості освітнього простору [24]. Узагальнюючи наукові підходи вважаємо, що технологічні критерії включають:

1) захищеність освітніх платформ від кібератак та несанкціонованого доступу;

2) наявність систем моніторингу соціальних мереж для виявлення

дезінформаційних компаній;

3) використання інструментів верифікації інформації та фактчекінгу;

4) ефективність систем захищеної комунікації між учасниками освітнього процесу;

5) впровадження штучного інтелекту для раннього виявлення патернів інформаційних атак.

Психологічні критерії стійкості характеризують емоційний та когнітивний стан учасників освітнього процесу, їхню здатність зберігати психологічну рівновагу та критичне мислення під впливом інформаційних загроз. А. Семеренко досліджує психологічну стійкість у контексті когнітивної війни, підкреслюючи її критичну важливість для прикордонних регіонів [72]. С. Максименко, І. Деркач та О. Ірхін аналізують теоретико-психологічні детермінанти когнітивних маніпуляцій, що дозволяє ідентифікувати ключові психологічні показники стійкості [35]. Систематизуючи наукові концепції виокремимо психологічні критерії, які охоплюють:

– рівень тривожності та стресу в освітній спільноті (що впливає на вразливість до маніпуляцій);

– ступінь довіри до офіційних джерел інформації та органів влади;

– наявність критичного мислення та скептицизму до непідтвердженої інформації;

– психологічна готовність до тривалого функціонування в умовах загрози;

– здатність до швидкого відновлення після інформаційних атак (резільєнтність).

В свою чергу, соціальні критерії стійкості відображають рівень згуртованості освітньої спільноти, наявність механізмів взаємопідтримки та ефективність горизонтальних зв’язків, що перешкоджають поширенню дезінформації. В. Сілайов підкреслює, що соціальна когезія є потужним захисним фактором проти когнітивних маніпуляцій [73]. Соціальні критерії включають:

– ступінь згуртованості педагогічного колективу та батьківської спільноти;

– наявність мереж взаємопідтримки в освітньому середовищі;

– швидкість розповсюдження достовірної інформації через неформальні канали;

– залученість громадських організацій до протидії дезінформації;

– рівень соціального капіталу освітньої спільноти.

Для систематизації розроблених критеріїв оцінки стійкості освітнього середовища та визначення конкретних показників їх вимірювання доцільно представити комплексну систему критеріїв у табличній формі, що дозволить забезпечити операціоналізацію теоретичних конструктів для практичного застосування (Таблиця 1.3).

Таблиця 1.3 – Критерії оцінки стійкості освітнього середовища до когнітивних маніпуляцій

Група критеріїв	*Показники*	*Методи вимірювання*	*Цільові значення*	*Частота моніторингу*
Інституційні	Наявність спеціалізованих підрозділів, розробленість НПА, функціонування систем раннього попередження	Аудит структури органів управління, аналіз документів, оцінка експертів	100% закладів охоплені системою моніторингу, час реагування <2 год	Щоквартально
Компетентнісні	Рівень медіаграмотності, навички цифрової гігієни, здатність до критичного мислення	Тестування, опитування, практичні завдання, спостереження	>80% педагогів з високим рівнем медіаграмотності, >70% учнів розпізнають маніпуляції	Двічі на рік
Технологічні	Захищеність платформ, системи моніторингу, інструменти верифікації, захищена комунікація	Технічний аудит, пентестинг, аналіз логів, оцінка спеціалістів	0 успішних кібератак, час виявлення фейків <1 год	Щомісячно
Психологічні	Рівень тривожності,	Психологічне тестування,	Рівень довіри до офіційних джерел	Щомісячно

	довіра до інституцій, критичне мислення, резільєнтність	опитування, інтерв'ю, спостереження	>70%, помірний рівень тривожності	
Соціальні	Згуртованість спільноти, взаємопідтримка, швидкість поширення достовірної інформації	Соціометрія, аналіз мереж, спостереження, опитування	Час поширення офіційної інформації <30 хв, рівень згуртованості >75%	Щоквартально

Джерело: розробка автора на основі [75, 27, 9, 31, 72].

Представлена система критеріїв забезпечує комплексну оцінку стійкості освітнього середовища до когнітивних маніпуляцій через вимірювання різних аспектів готовності та спроможності системи протидіяти інформаційним загрозам. Інтеграція інституційних, компетентнісних, технологічних, психологічних та соціальних критеріїв дозволяє отримати цілісне уявлення про стан безпеки освітнього простору регіону.

Цільові значення показників базуються на міжнародних стандартах та адаптовані до українських реалій з урахуванням специфіки воєнного стану. Регулярний моніторинг за визначеними критеріями дає можливість своєчасно виявляти зниження стійкості системи та коригувати протидійні заходи.

Особливо важливим є взаємозв’язок різних груп критеріїв, оскільки слабкість в одному аспекті автоматично знижує загальну стійкість системи незалежно від показників в інших сферах. Використання різноманітних методів вимірювання підвищує надійність оцінки та дозволяє триангулювати дані з різних джерел для перевірки достовірності результатів.

Підбиваючи підсумок, критичний аналіз представленої методології виявляє її сильні та слабкі сторони. Запропонована система критеріїв забезпечує комплексний підхід до оцінки стійкості освітнього середовища, інтегруючи інституційний, компетентнісний, технологічний, психологічний та соціальний виміри. Водночас постає питання практичної реалізації масштабного моніторингу в умовах обмежених ресурсів прикордонних регіонів. Деякі цільові

показники (наприклад, « 0 успішних кібератак») можуть бути надто амбітними для регіонів з недостатньою технічною інфраструктурою. Крім того, методологічні підходи значною мірою запозичені з міжнародного досвіду без достатньо адаптації до специфіки українського контексту та ресурсних можливостей.

Методологія аналізу ефективності механізмів публічного управління протидією інформаційним впливам вимагає інтеграції кількісних та якісних методів з урахуванням специфіки кризового контексту прикордонних регіонів. Триангуляція даних, лонгітюдний дизайн та порівняльний аналіз забезпечують достовірність результатів та можливість своєчасної корекції управлінських рішень.

Система критеріїв оцінки стійкості освітнього середовища до когнітивних маніпуляцій має охоплювати інституційні, компетентнісні, технологічні, психологічні та соціальні аспекти, забезпечуючи комплексний моніторинг готовності регіональної системи освіти до протидії інформаційним загрозам. Регулярне вимірювання показників за встановленими критеріями дозволяє органам публічного управління своєчасно коригувати стратегії захисту освітнього простору.

РОЗДІЛ 2
МІЖНАРОДНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ В ОСВІТІ

2.1 Кращі практики країн-членів НАТО щодо захисту освітнього простору

Аналіз міжнародного досвіду протидії гібридним загрозам в освітньому просторі демонструє, що країни-члени НАТО, особливо ті, які мають спільний кордон з Російською Федерацією або історичний досвід протистояння радянській експансії, розробили найбільш ефективні та випробувані практики захисту від інформаційних впливів. Країни Балтії (Естонія, Латвія та Литва) стали піонерами в розробці системних підходів до формування стійкості освітнього середовища, що базуються на власному травматичному досвіді п'ятдесятирічної радянської окупації (1940-1991) та тривалому інформаційному протистоянні з Російською Федерацією після відновлення незалежності.

Європейські дослідження підтверджують, що програми розвитку медіаграмотності в країнах НАТО демонструють послідовну інтеграцію критичного мислення в освітні системи як ключового елементу національної безпеки, що особливо виразно проявилося після анексії Криму 2014 року [56].

Крім того, стратегії протидії гібридним загрозам у публічному управлінні, розроблені у співпраці Європейського Союзу та України, підкреслюють критичну важливість адаптації європейських практик до специфіки пострадянського простору, де населення має низький рівень довіри до інституцій та високу вразливість до маніпулятивних наративів [59].

Естонський досвід захисту освітнього простору від інформаційних загроз є особливо релевантним для України через схожість історичного контексту, наявність значної російськомовної меншини (близько 25% населення) та

постійний інформаційний тиск з боку Російської Федерації. Після масштабних кібератак 2007 року, які частково були спрямовані на освітні інституції та паралізували роботу університетських серверів, Естонія створила одну з найбільш розвинених у світі систем цифрової безпеки в освіті. Естонська модель базується на трьох взаємопов'язаних принципах:

1) всеохоплююча цифрова грамотність населення з дитячого віку;

2) децентралізована система реагування на інформаційні загрози з високим ступенем автономії місцевих освітніх закладів;

3) безперервна співпраця між державними установами, освітніми закладами та технологічним сектором для розробки інноваційних рішень.

Дослідження Естонської моделі цифровізації освіти показують, що країна досягла найвищих показників цифрової безпеки серед країн ЄС завдяки інтеграції кібер захисту у національну стратегію безпеки на рівні конституційного пріоритету [26]. Флагманська програма «Tiger Leap», запроваджена ще в 1996 році та систематично оновлена у 2015-2020 роках відповідно до нових викликів гібридної війни, забезпечує інтеграцію цифрових навичок та критичного мислення в усі рівні освіти, від початкової школи до університетів. Особливої уваги заслуговує естонська практика обов'язкового навчання педагогів основам кібербезпеки та виявлення дезінформації, що передбачає регулярне оновлення компетенцій кожні два роки через сертифіковані курси від Національного центру кібербезпеки Естонії.

Латвійський підхід до протидії гібридним загрозам в освіті характеризується особливим акцентом на зміцненні національної ідентичності та активній протидії історичному ревізіонізму, що є критично важливим для прикордонних регіонів з історією радянської окупації, зокрема Латгальського регіону, де проживає до 60% російськомовного населення.

Латвійська стратегія інформаційної безпеки в освіті включає чотири взаємопов'язані компоненти:

1) обов'язкові курси національної історії з критичним аналізом радянської пропаганди та деконструкцією міфів про «визволення»;

2) програми захисту латиської мови та культури як елемента національної безпеки з обов'язковим вивченням історії латиської державності;

3) систему постійного моніторингу навчальних матеріалів на предмет виявлення прихованої пропаганди або маніпулятивного контенту;

4) спеціальні програми для шкіл національних меншин, що поєднують повагу до культурного розмаїття з формуванням Латвійської громадянської ідентичності.

Аналіз Латвійського досвіду виявляє, що Міністерство освіти і науки Латвії розробило унікальну цифрову платформу «ChecKit» для перевірки навчальних матеріалів, що дозволяє педагогам та батькам в режимі реального часу оцінювати якість та політичну нейтральність освітнього контенту [10]. Ця практика є вкрай актуальною для України, де після деокупації окремих територій Харківської, Херсонської та Донецької областей виникає гостра потреба в швидкій перевірці та оновленні навчальних програм, які протягом років окупації зазнали російської ідеологічної обробки.

Литовська модель протидії інформаційним загрозам базується на інноваційному принципі «активної стійкості» (active resilience), що передбачає не лише пасивні оборонні механізми, а й проактивні дії з формування критичного мислення та медіаграмотності всього населення, включаючи найвразливіші групи,- літніх людей та мешканців сільських територій. Литовське Міністерство освіти, науки та спорту розробило та впровадило національну програму медіаграмотності «Media Literacy and Critical Thinking», яка є обов'язковою для всіх рівнів освіти, від початкової школи до університетів та включає щотижневі практичні вправи з виявлення фейків, детального аналізу пропагандистських технік та верифікації інформації через множинні джерела.

Дослідження ефективності Литовської програми показують, що рівень розпізнавання маніпулятивного контенту серед учнів, які пройшли повний курс навчання, зріс з 45% до 80% протягом 2018-2023 років [40]. Особливістю Литовської програми є систематичне залучення журналістів-розслідників національних медіа та професійних фактчекерів з провідних організацій до

проведення щомісячних майстер-класів у школах та університетах, що забезпечує практичну орієнтованість навчання та знайомство учнів з реальними кейсами дезінформаційних компаній.

Литовський досвід також демонструє високу ефективність створення молодіжних груп «інформаційних захисників» (Debunk Squad), які активно протидіють дезінформації в соціальних мережах, освітніх онлайн-спільнотах та локальних месенджер-групах [40]. Ця низова ініціатива, що отримує організаційну та фінансову підтримку держави (близько 500 тис. євро щорічно з національного бюджету), створює горизонтальні мережі протидії, які виявляються значно ефективнішими за вертикальні адміністративні структури через швидкість реакції та природну довіру однолітків одне до одного.

Для систематизації та порівняння ключових характеристик балтійських практик доцільно представити комплексний аналіз стратегій Естонії, Латвії та Литви в табличній формі.

Таблиця 2.1 – Порівняльний аналіз практик країн Балтії щодо протидії гібридним загрозам в освіті

Країна	*Ключові елементи стратегії*	*Інституційна архітектура*	*Освітні програми*	*Технологічні рішення*	*Результати впровадження*	*Адаптивність для України*
Естонія	Цифрова грамотність, кіберзахист, державно-приватне партнерство	Національний центр кібербезпеки, координація з освітніми закладами	«Tiger Leap», обов'язкове навчання кібербезпеці педагогів (кожні 2 роки)	Захищені освітні платформи, ШІ для виявлення дезінформації	95% населення володіє цифровими навичками, мінімальна уразливість до кібератак	Висока: можливість адаптації технологічних рішень та програм підготовки педагогів
Латвія	Захист національної ідентичності, протидія історичному ревізіонізму	Міжвідомча комісія з моніторингу навчальних матеріалів	Курси національної історії з критичним аналізом пропаганди, захист мови	Платформа перевірки освітнього контенту, система моніторингу	Зниження впливу російської пропаганди на 70% (2015-2023)	Дуже висока: прямий досвід протидії подібним загрозам

Продовження таблиці 2.1

Країна	*Ключові елементи стратегії*	*Інституційна архітектура*	*Освітні програми*	*Технологічні рішення*	*Результати впровадження*	*Адаптивність для України*
Литва	Активна стійкість, проактивна протидія, залучення громадськості	Національна агенція з медіаграмотності, молодіжні групи захисників	«Media Literacy and Critical Thinking» (обов'язкова), майстер-класи від журналістів	Інструменти фактчекінгу для шкіл, мобільні додатки для перевірки інформації	80% учнів розпізнають маніпуляції, активна молодіжна мережа протидії	Висока: модель громадської активності відповідає українській традиції самоорганізації

Джерело: розробка автора на основі [26, 10, 40].

Аналіз досвіду країн Балтії виявляє чотири спільні паттерни (зразки) успішної протидії гібридним загрозам в освіті. По-перше, інтеграція медіаграмотності як наскрізної компетенції в усі освітні програми, а не як окремого ізольованого предмета, що забезпечує системність формування критичного мислення. По-друге, створення багаторівневої системи моніторингу та реагування, що гармонійно поєднує централізовані національні структури стратегічного рівня з гнучкою місцевою ініціативою на рівні громад та окремих освітніх закладів.

Дослідження Центру передового досвіду НАТО зі стратегічних комунікацій підтверджують, що постійне оновлення компетенцій педагогів відповідно до швидкої еволюції інформаційних загроз є третім критичним фактором успіху балтійських країн [28]. По-четверте, ефективне використання сучасних технологій, включаючи алгоритми штучного інтелекту та машинного навчання, для раннього виявлення координованих дезінформаційних кампаній до їх широкого розповсюдження в освітньому середовищі [83].

Критично важливим елементом балтійського успіху є те, що всі три країни розглядають інформаційну безпеку в освіті як питання національної безпеки найвищого рівня, закріплене в національних стратегіях безпеки поряд з військовою обороною та економічною стійкістю, що забезпечує необхідне

політичне та фінансове підґрунтя для реалізації довгострокових стратегій [14].

Для України особливо цінним є досвід Латвії щодо системної деколонізації освітнього простору та протидії історичному ревізіонізму, оскільки українська система освіти стикається з подібними викликами після десятиліть радянізації (1920-1991 рр.) та подальших спроб російської культурної експансії через контроль над освітнім контентом в окупованих регіонах Донбасу та Криму.

Фінський досвід протидії інформаційним загрозам в освіті базується на концепції «суспільної стійкості» (societal resilience), яка передбачає формування комплексної здатності суспільства протистояти кризам різного характеру, включаючи інформаційні атаки. Фінляндія, маючи 1300-кілометровий кордон з Росією та історичний досвід протистояння радянській агресії, розробила унікальну модель інтеграції критичного мислення в освітню систему, починаючи з дошкільної освіти. Фінська програма медіаграмотності не є окремим предметом, а інтегрована в усі дисципліни, від математики до фізкультури, що забезпечує наскрізний розвиток навичок критичного аналізу інформації.

Ключовим елементом фінського підходу є навчання дітей ставити правильні запитання до будь-якої інформації: хто автор, яка мета повідомлення, які докази надані, які альтернативні точки зору існують. Фінська модель також включає обов'язкове навчання педагогів протидії дезінформації як частину базової педагогічної освіти, а не як додаткове підвищення кваліфікації, що забезпечує системність підходу.

Польський досвід є цінним для України через схожість історичного контексту тривалого перебування під радянським впливом, спільну пострадянську спадщину деформованих інституцій та подібність структури освітніх систем, які обидві країни успадкували від радянської моделі [57]. Важливим кроком стало впровадження Польщею обов'язкового предмета «Media and Information Literacy» для учнів 7-9 класів у 2020 році, який включає систематичні практичні навички верифікації новин через перехресну перевірку джерел, критичний аналіз візуального контенту на предмет маніпуляцій та створення власних медіапроектів як форми активного громадянства.

Порівняльні дослідження європейських програм медіаграмотності виявили, що польська модель демонструє один з найвищих показників залученості учнів до активної протидії дезінформації [56]. Інноваційною особливістю польської моделі є створення національної мережі «шкіл фактчекерів», де учні старших класів (10-11 класи) навчаються професійним технікам перевірки інформації, використовуваним журналістами провідних польських медіа, та створюють власні дослідні проекти з розвінчання найпоширеніших дезінформаційних наративів про історію Польщі, ЄС та НАТО [50].

Американські практики підвищення інформаційної безпеки в освіті базуються на децентралізованій федеральній моделі, де кожен штат та навіть окремий шкільний округ має значну автономію в розробці власних програм протидії дезінформації відповідно до локальних потреб та політичного контексту [4]. Незважаючи на відсутність єдиної національної стратегії на федеральному рівні, американський досвід демонструє низку успішних локальних практик, що можуть бути критично переосмислені та адаптовані для українських реалій з урахуванням різниці політичних систем.

Найбільш масштабною є програма «News Literacy Project», яка з 2008 року охоплює понад 30 000 шкіл у 50 штатах США та навчає учнів фундаментальним навичкам відрізнення перевірених новин від реклами, пропаганди та розважального контенту [4]. Програма включає модулі з перевірки джерел інформації, розуміння етичних стандартів професійної журналістики та аналізу економічних моделей медіа, які впливають на якість контенту.

Американські дослідницькі університети, зокрема Стенфордський університет та Массачусетський технологічний інститут, активно залучають студентів бакалаврату та магістратури до міждисциплінарних досліджень феномену дезінформації та розробки інноваційних технологічних рішень для її автоматичного виявлення через аналіз великих даних [37]. Особливої уваги заслуговує досвід американських освітніх закладів у протидії внутрішнім загрозам інформаційній безпеці, таким як шкільний кібербулінг через соціальні

мережі або лавиноподібне розповсюдження неперевірених чуток про безпеку закладів, що може бути адаптовано для України в контексті боротьби з панікою та дезінформацією про загрози обстрілів.

Узагальнення досвіду провідних програм медіаграмотності країн НАТО дозволяє виокремити спільні методологічні підходи та оцінити їх потенціал адаптації для українського контексту.

Таблиця 2.2 – Програми медіаграмотності країн НАТО: порівняльна характеристика

Країна	*Назва програми*	*Цільова аудиторія*	*Ключові компоненти*	*Методологія*	*Фінансування*	*Виміряна ефективність*	*Можливість адаптації*
Фінляндія	«Critical Thinking in Education»	Дошкільна освіта – університет	Інтеграція в усі предмети, навчання правильним запитанням, аналіз джерел	Наскрізна компетенція, практичні завдання	Державний бюджет	90% населення має високий рівень медіаграмотності (EU Media Literacy Index)	Середня: потребує перебудови всієї освітньої системи
Польща	«Media and Information Literacy»	7-9 класи (обов'язково), факультативи для старших	Верифікація новин, аналіз візуального контенту, школи фактчекерів	Окремий курс + практика	Держава + НУО	65% учнів розпізнають фейки (2023), зростання на 35% за 3 роки	Висока: схожа освітня система та виклики
США	«News Literacy Project»	Середня та старша школа (30 000 закладів)	Відрізнення новин від пропаганди, перевірка джерел, етика журналістики	Факультативні курси, онлайн-платформа	Приватні фонди + корпорації	78% учасників покращили навички критичного аналізу	Середня: децентралізована модель складна для імплементації

Продовження таблиці 2.2

Країна	*Назва програми*	*Цільова аудиторія*	*Ключові компоненти*	*Методологія*	*Фінансування*	*Виміряна ефективність*	*Можливість адаптації*
Естонія	«Digital Competence Framework»	Всі рівні освіти	Цифрова безпека, кібергігієна, критичний аналіз онлайн-контенту	Інтегрований підхід + спецкурси	Державний бюджет	95% цифрової грамотності населення, найвищий показник у ЄС	Дуже висока: технологічні рішення легко адаптуються
Литва	«Media Literacy and Critical Thinking»	Початкова – старша школа (обов'язково)	Практичні вправи з фактчекінгу, молодіжні групи захисників, майстер-класи	Комбінований: теорія + практика + активізм	Держава + міжнародні гранти	80% учнів розпізнають маніпуляції, активна мережа 5000+ волонтерів	Висока: модель громадської активності близька до української

Джерело: розробка автора на основі [56, 80, 32, 37, 26, 40].

Порівняльний аналіз програм медіаграмотності країн НАТО виявляє п’ять критичних факторів успіху, які мають бути обов’язково враховані при розробці української стратегії протидії гібридним загрозам в освіті прикордонних територій.

По-перше, міжнародні дослідження однозначно демонструють, що найбільш ефективними виявляються програми, що органічно інтегровані в загальну освітню систему як наскрізна компетенція на всіх предметах, а не механічно ізольовані як окремий факультативний предмет [73]. Фінський та естонський досвід підтверджують перевагу інтегрованого підходу над дискретним.

По-друге, критично важливим для практичної ефективності навчання є систематичне залучення практиків-професіоналів: журналістів-розслідувачів національних медіа, експертів з фактчекінгу та спеціалістів з кібербезпеки до безпосереднього освітнього процесу [56]. Литовський досвід молодіжних

програм активної протидії показує, що залучення практиків збільшує мотивацію учнів та забезпечує актуальність навчального контенту [40].

По-третє, всі успішні національні програми обов’язково включають потужний технологічний компонент, надаючи учням та педагогам постійний доступ до сучасних інструментів верифікації інформації [76]. Системи моніторингу дезінформації в реальному часі є невід'ємною частиною інфраструктури освітньої безпеки [82].

По-четверте, найвищі показники ефективності протидії демонструють саме ті країни, де медіаграмотність офіційно визнана питанням національної безпеки найвищого рівня і відповідно фінансується на системному рівні з національних бюджетів безпеки [14]. Аналіз бюджетних пріоритетів країн НАТО підтверджує пряму кореляцію між рівнем фінансування та ефективністю програм.

По-п’яте, для України особливо актуальною є литовська модель активізації молоді як агентів низової протидії дезінформації, оскільки це органічно відповідає глибокій українській традиції громадської самоорганізації [69]. Така модель може бути швидко масштабована за відносно невеликих фінансових витрат через використання волонтерського потенціалу молоді [9].

Освітні програми НАТО для підвищення кібербезпеки включають широкий спектр спеціалізованих ініціатив, спрямованих на систематичну підготовку фахівців у сфері інформаційної безпеки та протидії гібридним загрозам як для країн-членів Альянсу, так і для держав-партнерів [73]. Флагманська програма «NATO Strategic Communications Centre of Excellence» (Stratcom COE), що функціонує в Ризі (Латвія) з 2014 року, розробила комплексну низку освітніх модулів для педагогів та адміністраторів освітніх закладів країн-партнерів, включаючи Україну.

Ці модулі охоплюють широкий тематичний спектр, від базової цифрової гігієни та захисту персональних даних до складних технік виявлення координованих дезінформаційних кампаній на ранніх стадіях їх розгортання [26]. Особливої уваги заслуговує інноваційна програма «Hybrid

Threats Education Platform», запущена у 2019 році, яка надає безкоштовний 24/7 доступ до інтерактивних навчальних матеріалів, реалістичних симуляцій гібридних атак та детальних кейс-стаді для освітян з усіх країн-партнерів НАТО [83].

Український досвід участі в цих міжнародних програмах з 2015 року демонструє їхню безсумнівну високу практичну цінність для підвищення компетенцій педагогів та управлінців [59]. Проте аналіз також виявляє критичну необхідність глибокої адаптації стандартних модулів до унікальної специфіки активного збройного конфлікту високої інтенсивності, оскільки абсолютна більшість навчальних матеріалів розроблена для країн, що не перебувають у стані повномасштабної війни [64].

Узагальнення міжнародного досвіду захисту освітнього простору від гібридних загроз демонструє, що найбільш сталих результатів досягають країни, які розробили та послідовно реалізують комплексні стратегії. Ці стратегії органічно інтегрують технологічні рішення для моніторингу загроз, освітні програми для формування компетенцій та інституційні механізми координації. Критичним фактором успіху виявляється наявність політичної волі на найвищому рівні та забезпечення стабільного багаторічного фінансування [64].

Підбиваючи підсумок, аналіз міжнародного досвіду виявляє три ключові виміри ефективних практик протидії гібридним загрозам в освіті:

Інституційний вимір характеризується визнанням інформаційної безпеки освіти пріоритетом національної безпеки на найвищому політичному рівні, що забезпечує стале фінансування та міжвідомчу координацію. *Методологічний* вимір передбачає інтеграцію медіаграмотності як наскрізної компетенції через усі рівні освіти, поєднуючи технологічні інструменти з педагогічними практиками формування критичного мислення. *Контекстуальний вимір* наголошує на необхідності адаптації міжнародних практик до національної специфіки, зокрема історичного досвіду, демографічних особливостей та ресурсних можливостей.

Досвід країн Балтії є найбільш релевантним для України через схожість

історичного контексту протидії російській інформаційній експансії. Естонська модель цифрової безпеки освіти демонструє ефективність технологічного підходу, латвійський досвід протидії історичному ревізіонізму надає практичні інструменти деколонізації освіти, литовська модель активної стійкості показує потенціал громадської мобілізації.

Фінська концепція всеохоплюючої безпеки та польський досвід пріоритезації прикордонних регіонів доповнюють балтійські практики. Для України критично важливим є синтез цих підходів з урахуванням специфіки воєнного стану, обмежених ресурсів та особливої вразливості прикордонних територій.

Успішність імплементації міжнародного досвіду залежатиме від здатності адаптувати глобальні практики до локальних умов при збереженні стратегічного фокусу на довгостроковому формуванні стійкості освітнього простору.

2.2 Вітчизняний досвід протидії інформаційним загрозам в освіті: аналіз практик регіонів України

Визначені у попередньому підрозділі кращі практики країн-членів НАТО щодо захисту освітнього простору створюють методологічну рамку для критичного аналізу вітчизняного досвіду протидії інформаційним загрозам в освітній сфері. Україна, перебуваючи в умовах повномасштабної війни, накопичила унікальний практичний досвід протидії інформаційним загрозам різної інтенсивності залежно від географічного розташування регіонів.

Розпорядженням Кабінету Міністрів України від 7 квітня 2023 р. № 301-р «Про схвалення Концепції безпеки закладів освіти» визначено стратегічне уявлення щодо безпечного освітнього середовища [58]. З одного боку, цей документ формує загальнонаціональну рамку безпеки освітнього простору, інтегруючи міжнародні стандарти захисту дітей в умовах конфлікту. З іншого

боку, критичний аналіз виявляє його концептуальність без деталізації конкретних механізмів адаптації до різних безпекових контекстів прикордонних, деокупованих та центральних областей. Це свідчить про типову для української державної політики проблему,- наявність стратегічного бачення за відсутності операційних інструментів його реалізації в умовах територіальної гетерогенності загроз.

Харківська область, безпосередньо межуючи з територією агресора, стала природним полігоном для відпрацювання інтенсивних практик формування медіаграмотності педагогічних працівників та учнів. Митнік С., аналізуючи досвід Харківської спеціалізованої школи №162, наголошує на необхідності інтеграції навичок інфо-медійної грамотності у навчальний процес початкової школи через формування критичного мислення та здатності верифікувати інформацію в режимі реального часу [39]. Водночас опитування педагогів, проведене MediaSapiens у 2023 році, показало, що східні прикордонні області виявили найвищу мотивацію вчителів до впровадження медіаграмотності через безпосереднє відчуття загрози дезінформації, проте саме ці регіони найменше забезпечені системною інституційною підтримкою [36].

Харківська модель демонструє високу адаптивність педагогічної спільноти до екстремальних умов, коли вчителі самостійно розробляють методики перевірки фактів і протидії маніпуляціям. Ця ініціативна природа практик створює критичний розрив між об’єктивними потребами та спроможністю освітньої системи. Понад 60% педагогів залишаються без базових компетенцій протидії інформаційним загрозам через відсутність обов’язкової сертифікації та фінансового стимулювання підвищення кваліфікації. Це дозволяє констатувати, що Харківський досвід, попри свою інноваційність, залишається фрагментованим і не масштабується через індивідуальний характер ініціатив окремих педагогів.

Сумська область розробила альтернативний підхід через реалізацію міжнародного проєкту «Медіаграмотність у регіонах України», організованого Interlink Academy за підтримки Посольства Німеччини. Студенти Конотопського

індустріально-педагогічного фахового коледжу СумДУ на чолі з викладачами пройшли інтенсивне навчання тренінговим методам протидії пропаганді, маніпуляціям та фейкам, формуючи мережу майбутніх агентів змін у освітньому просторі громад [41]. Порівняльний аналіз Харківської та Сумської моделей виявляє принципову різницю підходів. Якщо Харківські практики формуються «знизу» як відповідь на безпосередню загрозу, то Сумська модель базується на каскадному механізмі поширення компетенцій через систематичну підготовку тренерів.

З одного боку, Сумська модель демонструє прогресивність у створенні мультиплікаційного ефекту, коли підготовлені педагоги стають провідниками медіаграмотності у своїх громадах. З іншого боку, критичний аналіз виявляє типову для України залежність від міжнародного грантового фінансування, що ставить під питання сталість ініціативи після завершення проєкту та відсутність механізмів інтеграції набутих компетенцій у формальну систему атестації педагогів.

Отже, можна стверджувати, що східні регіони демонструють високу інтенсивність локальних практик при критично низькій системності та інституційному закріпленні напрацювань, що вимагає переходу від проєктної логіки до державної політики обов’язкової медіаосвіти.

Миколаївська та Херсонська області, перебуваючи в зоні активних бойових дій та часткової деокупації, демонструють унікальну практику інтеграції заходів фізичної та інформаційної безпеки освітніх закладів. За даними Міністерства освіти і науки України, у цих областях активно зводяться підземні освітні простори, які створюються не лише як укриття під час обстрілів, але й як повноцінні навчальні середовища з облаштуванням технологічної інфраструктури для дистанційної освіти [78]. Цей підхід, на перший погляд, виглядає як комплексне рішення проблеми безпеки освітнього процесу в умовах війни.

Водночас критичний аналіз виявляє непередбачені ефекти такого рішення. Інвестиції у фізичну безпеку демонструють пріоритетність збереження життя

учнів і педагогів, що безумовно є першочерговим завданням держави. В той же час, фокус на фізичній безпеці часто відволікає обмежені ресурси від інформаційного виміру загроз, коли батьки та учні отримують дезінформацію про небезпеку навчання через соціальні мережі значно швидше, ніж адміністрація закладів встигає її спростувати. Це створює парадоксальну ситуацію, коли наявність захищеної інфраструктури не гарантує її використання, якщо населення дезінформоване щодо реальних ризиків і переваг офлайн навчання.

Досвід деокупації Херсона виявив специфічні виклики, які принципово відрізняються від загроз у прикордонних регіонах, що ніколи не були під окупацією. Міністерство внутрішніх справ України наголошує на критичній важливості стабілізаційних заходів, включаючи безпеку громадян та розмінування, проте залишає поза увагою необхідність психологічної деокупації та відновлення медіаграмотності населення [20]. Дослідження Центру інноваційної освіти «Про.Світ» виявляє фундаментальні проблеми закладів загальної середньої освіти на деокупованих територіях, зокрема, вплив окупаційної пропаганди на дітей, їхнє ставлення до вчителів з різним досвідом окупації, кадрові проблеми через колаборантську діяльність частини освітян та необхідність формування проукраїнської екосистеми в освітніх закладах [51].

Таким чином, державна політика коректно визначає пріоритет фізичної безпеки та відновлення інфраструктури на деокупованих територіях. В той же час, критичний аналіз свідчить, що класичні підходи до протидії дезінформації, ефективні в центральних регіонах, виявляються недостатніми в умовах, коли потрібна реінтеграція населення в український інформаційний простір після тривалого відриву.

Отже, південні регіони потребують не стандартних програм медіаграмотності, а спеціалізованих методик деколонізації свідомості, які враховують травматичний досвід окупації та формують стійкість до повторних інформаційних впливів. Це вимагає розробки окремого напряму державної політики, який поєднує психологічну підтримку з медіаосвітою.

Вінницька область, не перебуваючи під безпосередньою загрозою окупації, розробила превентивну модель формування медіаграмотності через проведення Всеукраїнського уроку медіаграмотності з елементами ігрової механіки та розіграшем призів для шкіл-переможців [21`]. Цей підхід одночасно демонструє креативність у залученні учнів до вивчення медіаграмотності через геймифікацію навчального процесу, що може підвищувати мотивацію молоді одночасно із ризиком поверхневості одноразових заходів, коли медіаграмотність перетворюється на разову акцію замість системної роботи впродовж навчального року, формуючи у школярів ілюзію володіння компетенціями без їх реального засвоєння.

Міністерство освіти і науки України підтримує загальнодержавну ініціативу впровадження медіаграмотності, наголошуючи, що вона викладається як у формі окремих курсів, так і інтегровано в межах базових предметів [42]. Однак, співставлення офіційної позиції Міністерства освіти і науки України з реальними практиками регіонів виявляє фундаментальну суперечність через те, що декларована підтримка на національному рівні фактично не супроводжується обов’язковістю викладання та єдиними стандартами якості. Це призводить до надзвичайної варіативності від систематичних курсів у передових школах столиці до повної відсутності медіаосвіти в периферійних закладах Закарпаття чи Кіровоградщини.

Фактично, українська система освіти демонструє модель «двох швидкостей», де якість медіаосвіти визначається не об’єктивними потребами регіону, а наявністю локальних ентузіастів і доступом до міжнародних проєктів.

Львівська область демонструє високу активність громадських організацій у протидії дезінформації через освітні ініціативи. Школа №90 міста Львова реалізувала проєкт від Офісу доброчесності Національного агентства з питань запобігання корупції «Прозора школа», в рамках якого учні 6-х, 9-х, 10-х, 11-х класів навчалися визначати дезінформацію та поводитися доброчесно онлайн [84]. З одного боку, львівська практика ілюструє силу громадянського суспільства в компенсації державних прогалин через проєктні ініціативи. З

іншого боку, ця модель виявляє типову для західних регіонів залежність від проактивності третього сектору, коли громадські організації фактично виконують функції держави у сфері медіаосвіти.

Центр стратегічних комунікацій та інформаційної безпеки, реалізуючи підхід «whole-of-society» до протидії дезінформації, провів за період з лютого 2022 по жовтень 2024 року майже 200 тренінгів для понад 1700 державних службовців, формуючи критичну масу фахівців здатних протидіяти інформаційним впливам [60]. Аналіз географічного розподілу цих тренінгів виявив парадоксальну закономірність: найбільш активна робота з медіаграмотності здійснюється в регіонах з найнижчою інтенсивністю інформаційних загроз (Київ, Львів, Івано-Франківськ), тоді як східні прикордонні території, попри найвищі ризики, отримують непропорційно менше системної підтримки через обмежені адміністративні ресурси в умовах воєнного стану.

Таким чином, можна констатувати, що центральні та західні регіони створюють якісні локальні ініціативи, які, проте, не масштабуються на всю країну через проєктну логіку фінансування та відсутність державних механізмів тиражування успішних практик.

Міжнародний проєкт Erasmus+ «Academic Response to Hybrid Threats» (WARN), реалізований консорціумом українських та європейських університетів у 2019-2023 роках, став унікальною спробою створення транссекторального академічного середовища для підвищення цивільної стійкості до гібридних загроз [1]. Національний університет «Острозька академія» наголошує, що проєкт спрямований на оновлення навчальних програм у семи галузях знань через впровадження унікального контенту про гібридні загрози та інноваційні геймифіковані методи викладання на основі штучного інтелекту [3].

Університет Ювяскюля (Фінляндія) як координатор проєкту визначає його мету: заповнити розрив у навичках безпеки в різних професійних галузях через підготовку «агентів позитивних змін», здатних проактивно адаптуватися до нових складних гібридних викликів та поширювати знання в суспільстві [2].

Проєкт WARN демонструє можливості міжнародної академічної кооперації у відповідь на гібридні загрози, створюючи високоякісний освітній контент і методології викладання на рівні вищої освіти. Але критичний аналіз цього документу виявляє типову для академічних ініціатив проблему,- створення складного теоретичного апарату аналізу гібридних загроз не трансформується автоматично в практики шкільної медіаосвіти, де потреби є найбільш гострими. Університетські курси з протидії гібридним загрозам залишаються недоступними для вчителів шкіл, які потребують не теоретичних рамок, а простих, практичних інструментів верифікації інформації для щоденного використання в класі.

Більше того, аналіз географічного розподілу університетів-учасників проєкту виявляє його концентрацію у великих містах (Київ, Харків, Острог), тоді як сільські та малі міські школи залишаються поза охопленням академічних напрацювань. Отже, критичний розрив між академічним сектором, що розробляє складні теоретичні рамки гібридних загроз, та школами прикордонних територій, які потребують негайних практичних рішень. Це вимагає створення «перекладацьких» механізмів, які б адаптували академічні напрацювання до рівня шкільної освіти через розробку методичних посібників, тренінгових модулів та цифрових платформ, доступних для педагогів без спеціалізованої підготовки з питань безпеки.

Порівняльний аналіз регіональних практик протидії інформаційним загрозам в освіті виявляє фундаментальну неоднорідність підходів, зумовлену не стільки об’єктивними відмінностями безпекового контексту, скільки різницею в адміністративному потенціалі, доступі до ресурсів та історико-культурних особливостях територій. Декларація про безпеку шкіл, до якої Україна приєдналася у 2019 році як сота країна, визначає міжнародні зобов’язання щодо попередження нападів на заклади освіти та їх використання у військових цілях [18]. Розпорядження Кабінету Міністрів України від 4 серпня 2021 р. затвердило план заходів щодо реалізації цієї Декларації [79].

Gриєднання до Декларації продемонструвало готовність України

дотримуватися міжнародних стандартів захисту освітніх закладів в умовах конфлікту. Проблемним питанням залишається лише теб, що імплементація цих принципів в українському контексті зосереджена переважно на фізичній безпеці (будівництво укриттів, евакуаційні процедури), тоді як інформаційний вимір загроз залишається недооціненим у державній політиці. Це проявляється у відсутності окремої статті фінансування програм медіаграмотності в освітніх бюджетах регіонів та необов'язковості цієї компетенції для атестації педагогічних працівників. Фактично, держава демонструє реактивний підхід до інформаційних загроз, зосереджуючись на фізичній безпеці як більш очевидній і вимірюваній проблемі.

Резюмуючи аналіз вітчизняного досвіду протидії інформаційним загрозам в освіті, можна констатувати формування різноманітного ландшафту регіональних практик, кожна з яких має власні сильні сторони та системні обмеження. Східні прикордонні регіони демонструють найвищу мотивацію до впровадження медіаграмотності через безпосереднє відчуття загрози, проте страждають від критичної відсутності системності та інституційного закріплення напрацювань, що трансформує індивідуальний героїзм педагогів у нестійку практику без довгострокового впливу.

Південні деокуповані території виявляють специфічні потреби в методиках психологічної деокупації та реінтеграції населення в український інформаційний простір, які не задовольняються стандартними програмами медіаосвіти, розробленими для регіонів без досвіду окупації. Центральні та західні регіони, маючи значно кращий доступ до ресурсів та міжнародних проєктів, створюють якісні локальні ініціативи, які, проте, не масштабуються на всю країну через проєктну логіку фінансування та відсутність державних механізмів тиражування успішних практик, формуючи модель «острівців успіху» в океані неохоплених територій.

Проєкт WARN як академічна ініціатива продемонстрував можливості транссекторальної співпраці, водночас виявив критичний розрив між університетськими розробками та потребами шкільної освіти. Отже, вітчизняний

досвід протидії інформаційним загрозам в освіті характеризується високою локальною інноваційністю за відсутності загальнонаціональної системності, що визначає необхідність створення спеціалізованих механізмів адаптації академічного знання та локальних практик до єдиної системи протидії інформаційним загрозам на рівні закладів загальної середньої освіти прикордонних територій, детальний аналіз яких буде здійснено у наступному розділі дослідження.

РОЗДІЛ 3
ПРАКТИЧНІ МЕХАНІЗМИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ В СИСТЕМІ ОСВІТИ ХАРКІВСЬКОЇ ОБЛАСТІ

3.1 Аналіз сучасного стану та вразливостей освітньої системи Харківської області

Харківська область як прикордонний регіон, що зазнав окупації північних районів у перші місяці повномасштабного вторгнення та продовжує перебувати під постійною загрозою ракетних обстрілів, демонструє унікальну конфігурацію викликів для системи освіти, що поєднує фізичну небезпеку з інтенсивним інформаційним тиском [19]. Освітня мережа регіону станом на 2025/2026 навчальний рік налічує понад 800 закладів загальної середньої освіти [45]. Крім того, в області функціонує близько 50 закладів вищої освіти, які працюють в екстремальних умовах, коли необхідність забезпечення безперервності навчального процесу поєднується з критичними викликами безпеки [55].

Особливості організації освітнього процесу у Харківській області включають феномен «підземних шкіл», спеціально обладнаних навчальних просторів у підвалах та на станціях метро, що стали символом стійкості Харківської освітньої спільноти [19]. Проте водночас ці інноваційні освітні простори створили нові вразливості для інформаційних атак та психологічного тиску через інтенсивне міжнародне медійне висвітлення [11].

Моніторинг організації освітнього процесу в умовах воєнного стану, здійснюваний Харківською обласною військовою адміністрацією, виявляє системні проблеми в забезпеченні фізичної безпеки освітніх закладів [44]. Водночас інформаційна безпека учасників освітнього процесу залишається недостатньо захищеною, що створює додаткові ризики для освітньої спільноти [5].

Характеристика освітньої мережі Харківської області станом на початок 2025/2026 навчального року демонструє драматичні зміни, спричинені повномасштабною війною та її наслідками для регіону. За офіційними даними Департаменту науки і освіти Харківської обласної військової адміністрації, загальна кількість закладів загальної середньої освіти скоротилася з 887 у 2021 році до 823 у 2025 році [55]. Це скорочення відбулося внаслідок руйнування інфраструктури та неможливості функціонування закладів у деокупованих та прифронтових районах [5].

Охоплення учнів очною формою навчання становить лише 38% від довоєнного рівня [45]. Водночас 52% учнів навчаються дистанційно, а 10% – у змішаному форматі, що створює принципово нові виклики для системи публічного управління освітою [67]. Особливістю Харківської освітньої мережі є функціонування 47 підземних навчальних просторів. З них 12 розташовані на станціях метрополітену, 28 в обладнаних підвалах шкіл [19]. Ще 7 підземних освітніх просторів створено у спеціально побудованих укриттях, що дозволяє частково відновити очне навчання навіть під час повітряних тривог [11]. Проте ця інноваційна практика, широко висвітлена в міжнародних медіа як приклад стійкості української освіти, парадоксально створила нові точки вразливості для інформаційних атак, про що буде детальніше йтися далі [22].

Кадрова ситуація в освітній сфері Харківської області характеризується критичним дефіцитом педагогічних працівників, посиленим масовою евакуацією населення на початку повномасштабної війни та триваючим стресом від роботи в умовах постійної загрози. Станом на жовтень 2025 року в регіоні бракує близько 2800 вчителів, що становить 18% від необхідної кількості, при цьому найгостріший дефіцит спостерігається саме в прифронтових районах, де освітні заклади потребують найбільшої підтримки [5].

Середній вік педагогічних працівників зріс до 48 років, що відображає відтік молодих спеціалістів з регіону та проблеми з залученням нових кадрів в умовах воєнного стану [55]. Критично важливим аспектом є те, що лише 23% вчителів пройшли спеціалізоване навчання з медіаграмотності та виявлення

дезінформації [44]. Це робить педагогічну спільноту вразливою до інформаційних маніпуляцій та обмежує можливості формування критичного мислення учнів [66]. Психологічне вигорання педагогів, які працюють в умовах постійного стресу, поєднуючи викладацьку діяльність з необхідністю забезпечення безпеки дітей під час обстрілів, створює додаткову вразливість до когнітивних впливів [61]. Хронічний стрес знижує здатність педагогів до критичного аналізу інформації, що є додатковим фактором ризику в умовах інтенсивних інформаційних атак [66].

Технічна інфраструктура для дистанційного навчання в Харківській області розвивалася форсованими темпами з початку повномасштабної війни, проте залишається недостатньою для забезпечення якісної освіти та захисту від інформаційних загроз. Міністерство освіти і науки України затвердило Типову освітню програму для дистанційного навчання, що стала основою для організації освітнього процесу в регіоні [43]. Проте її впровадження стикається з численними технічними та організаційними викликами [48].

Освітні заклади області активно використовують сучасні цифрові платформи та електронні ресурси для забезпечення безперервності навчання [53]. Координація дій між адміністраціями закладів, батьками, педагогами та місцевою владою спрямована на забезпечення рівного доступу до освіти в умовах змішаних та дистанційних форм навчання [48]. Водночас лише 34% освітніх закладів мають спеціалізоване програмне забезпечення для захисту від кібератак та несанкціонованого доступу [77]. Проблема нестабільного інтернет-з'єднання, особливо в сільських районах та під час обстрілів енергетичної інфраструктури, створює «вікна вразливості», коли учні та педагоги змушені використовувати менш захищені канали комунікації або звертатися до неперевірених джерел інформації [23].

Відсутність єдиної регіональної системи захищеної комунікації для освітньої спільноти робить можливими фішингові атаки та розповсюдження фейкових повідомлень від імені адміністрації закладів [23]. Це створює сприятливі умови для інших форм інформаційних маніпуляцій, які підривають

довіру до офіційних джерел комунікації [33].

Аналіз даних виявляє критичну залежність між фізичними наслідками війни для освітньої інфраструктури та вразливістю системи до інформаційних загроз, що створює ефект подвійного ураження освітньої спільноти. Скорочення кількості функціонуючих закладів та концентрація учнів у меншій кількості шкіл означає, що успішна інформаційна атака на один заклад може вплинути на значно більшу кількість дітей та їхніх родин, створюючи ефект масштабування загроз.

Драматичне зростання частки дистанційного навчання з епізодичного явища до домінуючої форми організації освітнього процесу фундаментально змінило характер вразливостей, перемістивши їх з переважно фізичного простору школи в цифрове середовище, де контроль за інформаційними потоками є значно складнішим. Феномен підземних шкіл, будучи вимушеною інновацією для забезпечення безперервності очного навчання, парадоксально створив нові точки вразливості. Інтенсивне міжнародне медійне висвітлення зробило ці об’єкти помітними цілями для цільової дезінформації про їхню безпеку з метою деморалізації населення.

Катастрофічне зростання дефіциту педагогічних кадрів з 2,2% до 18% не є просто кількісною проблемою, а створює якісно нову ситуацію, коли перевантажені та психологічно виснажені вчителі фізично не здатні приділяти достатню увагу розвитку критичного мислення учнів та виявленню інформаційних маніпуляцій. Особливо тривожним є той факт, що лише 23% педагогів пройшли навчання з медіаграмотності, що означає, що абсолютна більшість вчителів не володіє необхідними компетенціями для захисту учнів від когнітивних маніпуляцій та формування їхньої інформаційної стійкості.

Виявлені канали інформаційного впливу на освітню спільноту Харківської області демонструють еволюцію тактик гібридної війни, що адаптувалися до специфіки прикордонного регіону в умовах активних бойових дій. Дослідження каналів інформаційного впливу, проведене у 2023-2024 роках, виявило, що основними платформами для розповсюдження дезінформації стосовно освітніх

закладів є Telegram, який використовується у 68% зафіксованих випадків. Facebook використовується у 21% випадків інформаційних атак. Месенджер Viber застосовується у 7% випадків, а інші месенджери у 4% зафіксованих інцидентів [52].

Специфіка Telegram як домінуючого каналу пояснюється його популярністю серед українських користувачів для отримання оперативної інформації про повітряні тривоги та безпекову ситуацію [52]. Це створює довіру до контенту на цій платформі та робить її привабливою для розповсюдження дезінформації [22].

Найпоширенішими типами інформаційних атак є фальшиві повідомлення про обстріли конкретних шкіл, які становлять 42% випадків [5]. Маніпуляції з графіками роботи навчальних закладів складають 28% зафіксованих інцидентів [22]. Дезінформація про безпеку підземних навчальних просторів становить 18% випадків [19]. Фейкові розпорядження від імені освітніх органів складають 12% інформаційних атак [22].

Соціальні мережі та месенджери функціонують як подвійний інструмент: одночасно будучи необхідними каналами офіційної комунікації в умовах війни та платформами для розповсюдження дезінформації, що створює складний виклик для системи публічного управління освітою. Харківська освітня спільнота активно використовує Telegram-канали для оперативного інформування про повітряні тривоги, зміни в розкладі занять та організаційні питання [52]. Проте ця залежність від месенджерів створила вразливість до створення фейкових каналів, що імітують офіційні джерела [22].

Типовою тактикою інформаційних атак є створення Telegram-каналів з назвами, схожими на офіційні канали шкіл або управлінь освіти (наприклад, «Школа №15 ОФІЦІЙНО» замість «Школа №15 Харків»), які публікують дезінформацію про загрози безпеці або зміни в організації навчального процесу [22]. Facebook використовується для таргетованих атак на батьківські спільноти через створення фейкових акаунтів «стурбованих батьків» [52]. Ці акаунти розповсюджують паніку щодо безпеки конкретних шкіл або критикують

адміністрацію за нібито недостатні заходи безпеки.

Viber-групи класів та батьківських комітетів, будучи менш публічними, стають платформами для розповсюдження неперевірених чуток. Через довірливі стосунки між учасниками груп такі чутки поширюються швидше та сприймаються некритично [52].

Дезінформація про безпеку освітніх закладів становить найбільш небезпечний тип інформаційного впливу, оскільки безпосередньо впливає на рішення батьків про відправлення дітей до школи та психологічний стан усієї освітньої спільноти. Аналіз інформаційних інцидентів у Харківській області протягом 2023-2025 років виявив 387 зафіксованих випадків розповсюдження недостовірної інформації про загрози конкретним освітнім закладам [5]. При цьому 73% з них були ідентифіковані як навмисна дезінформація, а не помилкові повідомлення [22].

Найбільш резонансним випадком став інцидент у березні 2024 року, коли координована атака через Telegram розповсюдила фальшиві повідомлення про нібито заплановані обстріли всіх підземних шкіл Харкова. Це призвело до паніки серед батьків та зриву навчального процесу в 34 закладах на три дні, незважаючи на оперативні спростування від Харківської обласної військової адміністрації [22].

Дезінформація про підземні школи експлуатує природний страх батьків за безпеку дітей у закритих підземних просторах [19]. Вона використовує емоційно забарвлений контент про нібито недостатню вентиляцію, ризики обвалу або неможливість евакуації [22]. Маніпуляції з графіками роботи освітніх закладів, включаючи фальшиві повідомлення про скасування занять або перехід на дистанційний формат, створюють хаос в організації освітнього процесу [5]. Такі маніпуляції підривають довіру до офіційних каналів комунікації та дезорганізують роботу освітньої системи [22].

Психологічний стан освітньої спільноти Харківської області, який характеризується хронічним стресом від життя під постійною загрозою обстрілів, є критичним фактором вразливості до когнітивних маніпуляцій та

інформаційних впливів. За даними Звіту про діяльність із психологічної підтримки освітян та населення Харківської області за 2024 рік, Харківська регіональна психологічна служба здійснила 49 виїзних заходів до 27 територіальних громад області, охопивши 1418 осіб, серед яких 280 батьків з дітьми та підлітками [81].

За результатами діяльності Центру практичної психології КВНЗ «Харківська академія неперервної освіти», протягом 2024 року тематичними вебконсультаціями з профілактики стресу та першої психологічної допомоги було охоплено 526 педагогічних працівників [81]. Крім того, 103 практичних психологи пройшли курси підвищення кваліфікації за темою «Процедури і техніки консультування в роботі фахівців психологічної служби з урахуванням сучасних викликів». В області функціонують 25 мобільних бригад психосоціальної допомоги, з яких 13 працюють за підтримки міжнародних організацій UNFPA, УВКБ ООН та Corus International [81]. Водночас значна частина педагогів продовжує відчувати симптоми професійного вигорання та тривожних розладів, що знижує їхню здатність критично оцінювати інформацію [70].

Ці психологічні стани створюють ідеальні умови для когнітивних маніпуляцій, оскільки люди в стані хронічного стресу та тривожності є більш вразливими до емоційно забарвленого контенту [61]. Вони схильні приймати рішення імпульсивно та менш здатні до критичного аналізу інформації [66]. Програми психологічної підтримки учнів та педагогів, реалізовані в рамках Всеукраїнської програми ментального здоров’я «Ти як?», включають 83 індивідуальних та 48 групових сесій, проведених Харківською регіональною психологічною службою у 2024 році [81]. Проте ці програми зосереджені переважно на подоланні травми та стабілізації емоційного стану і майже не включають компонент формування когнітивної стійкості до інформаційних маніпуляцій, що є критичною прогалиною в системі психологічної підтримки [61].

Систематизація зафіксованих інформаційних інцидентів у Харківській

області протягом 2023-2025 років дозволяє виокремити основні типи загроз, їхні характеристики та наслідки для функціонування освітньої системи в табличній формі.

Таблиця 3.1 – Типологія інформаційних загроз для освітньої системи Харківської області (2023-2025)

Тип загрози	*Частота випадків*	*Основні канали*	*Цільові групи*	*Типові наративи*	*Середній час спростування*	*Наслідки*
Фейки про обстріли шкіл	163 (42%)	Telegram (78%), Facebook (15%), Viber (7%)	Батьки, педагоги	«Сьогодні вночі обстріляли школу №X», «Завтра планують атаку на район Y»	2-4 години	Паніка, масові звернення до адміністрації, зрив навчального процесу
Маніпуляції з графіками	108 (28%)	Фейкові Telegram-канали (65%), Viber-групи (25%), SMS (10%)	Учні, батьки, вчителі	«Завтра навчання скасовано», «Всі переходять на дистанційку з понеділка»	1-3 години	Дезорганізація процесу, навантаження на адміністрацію для з’ясування
Дезінформація про підземні школи	70 (18%)	Facebook (45%), Telegram (35%), YouTube (20%)	Батьки, міжнародна аудиторія	«У підвалах немає кисню», «Діти задихаються під землею», «Небезпечно евакуюватися»	4-6 годин	Відмова батьків відправляти дітей, міжнародний резонанс
Фейкові розпорядження	46 (12%)	Підроблені документи в Telegram (60%), Email (25%), фейкові	Педагоги, адміністрація	Накази про закриття закладів, зміну форми навчання, обов’язкову евакуацію	3-5 годин	Плутанина в організації, втрата довіри до офіційних документів

		сайти (15%)				
Атаки на керівництво	32 (8%)	Facebook (55%), Telegram (30%), коментарі на новинних сайтах (15%)	Громадськість, батьки	Звинувачення адміністрації у недбалості, корупції, неадекватних рішеннях	6-12 годин	Підрив довіри до керівництва, демотивація педагогів

Продовження таблиці 3.1

Тип загрози	*Частота випадків*	*Основні канали*	*Цільові групи*	*Типові наративи*	*Середній час спростування*	*Наслідки*
Провокації на мовному ґрунті	18 (5%)	Facebook (50%), Telegram (40%), Twitter/X (10%)	Вся спільнота	Конфлікти навколо мови навчання, звинувачення у дискримінації	12-24 години	Розкол спільноти, відволікання від реальних проблем

Джерело: складено автором на основі [5; 22; 52]

Наведені дані демонструють, що інформаційні загрози характеризуються високою частотою, різноманітністю каналів поширення та значними деструктивними наслідками для організації освітнього процесу, що визначає необхідність розробки комплексних механізмів протидії.

Аналіз типології інформаційних загроз виявляє чітку кореляцію між типом загрози та швидкістю її спростування, що демонструє недостатність існуючих механізмів оперативного реагування в системі публічного управління освітою Харківської області. Найбільш поширений тип загроз фейки про обстріли конкретних шкіл, характеризується відносно швидким спростуванням (2-4 години), проте цей час є надто тривалим, оскільки за ці години дезінформація встигає викликати паніку та масові звернення до адміністрації, які паралізують роботу закладів.

Маніпуляції з графіками навчання, хоча і спростовуються швидше (1-3 години), створюють максимальну дезорганізацію, оскільки впливають на щоденне планування тисяч родин та вимагають індивідуальних з'ясувань через множинні канали комунікації. Дезінформація про підземні школи є найбільш складною для спростування (4-6 годин) через емоційну забарвленість теми та залучення міжнародної аудиторії, яка часто не має доступу до українських офіційних джерел та покладається на контент у соціальних мережах.

Фейкові розпорядження, незважаючи на їхню меншу частоту, є особливо небезпечними через створення плутанини на інституційному рівні та підрив

довіри до офіційних документів, що може мати довгострокові наслідки для ефективності публічного управління. Атаки на керівництво освітніх закладів та органів управління освітою, хоча і становлять лише 8% від загальної кількості інцидентів, характеризуються найповільнішим спростуванням (6-12 годин) та найбільш руйнівним впливом на довіру до інституцій, що є стратегічною метою гібридної війни.

Аналіз діяльності Департаменту науки і освіти Харківської обласної військової адміністрації щодо протидії інформаційним загрозам виявляє значний розрив між масштабом викликів та адекватністю інституційної відповіді, що залишає освітню систему регіону вразливою до інформаційних маніпуляцій [55]. Департамент, будучи ключовим органом публічного управління освітою в регіоні, зосереджений переважно на вирішенні питань фізичної безпеки освітніх закладів, організації евакуації, відновлення зруйнованої інфраструктури та забезпечення безперервності навчального процесу. Водночас інформаційна безпека залишається периферійним питанням без окремого підрозділу та спеціалізованих фахівців [5].

У структурі Департаменту відсутня спеціалізована служба моніторингу інформаційних загроз та оперативного реагування на дезінформацію [55]. Це призводить до ситуації, коли спростування фейків здійснюється несистемно, часто з запізненням, через загальний відділ комунікації, що одночасно відповідає за десятки інших функцій [33].

Координація між Департаментом, Службою безпеки України, Національною поліцією є епізодичною та реактивною, активізуючись лише після масштабних інцидентів [33]. Також обмеженою є взаємодія з Центром протидії дезінформації при Раді національної безпеки і оборони України [7]. Замість функціонування як постійно діючий механізм превентивного моніторингу та швидкого реагування, ця координація залишається фрагментарною [33].

Моніторинг організації освітнього процесу, який здійснює Харківська обласна військова адміністрація, включає показники охоплення учнів різними формами навчання, стан матеріально-технічної бази, забезпечення закладів

педагогічними кадрами. Проте він не включає систематичного відстеження інформаційних загроз, рівня медіаграмотності учасників освітнього процесу або ефективності комунікаційних каналів [5].

Річний план роботи Департаменту освіти на 2025 рік містить загальні формулювання про необхідність «забезпечення інформаційної безпеки» та «протидії негативним інформаційним впливам» [55]. Проте він не включає конкретних заходів, ресурсного забезпечення, відповідальних осіб та показників ефективності, що перетворює ці декларації на формальність без реального впливу.

Розвиток системи моніторингу інформаційних загроз на регіональному рівні, який міг би забезпечити раннє виявлення дезінформаційних кампаній та координацію протидійних заходів, залишається на стадії обговорення без конкретних кроків до впровадження [49]. Захищені канали комунікації у системі освіти Харківщини, які могли б мінімізувати ризики розповсюдження фейкових повідомлень від імені офіційних органів, не створені. Вся комунікація здійснюється через загальнодоступні платформи без належної верифікації відправників, що залишає систему вразливою до інформаційних атак [23].

Результати опитування педагогів та учнів щодо рівня медіаграмотності та досвіду зіткнення з дезінформацією демонструють критичну недостатність компетенцій для протидії інформаційним маніпуляціям у значної частини освітньої спільноти. Опитування, проведене у 2024 році серед 1850 педагогів та 3200 учнів 8-11 класів з різних районів Харківської області, виявило тривожні результати щодо рівня медіаграмотності [22].

Серед вчителів лише 31% можуть правильно ідентифікувати всі ознаки маніпулятивного контенту в тестових завданнях [22]. Водночас 42% педагогів ідентифікують частину ознак маніпуляцій. Крім того, 27% вчителів демонструють низький рівень розпізнавання інформаційних маніпуляцій [66]. Серед учнів результати ще більш тривожні: лише 18% можуть критично проаналізувати інформацію та перевірити її достовірність [22]. При цьому 35% школярів роблять це частково. Найбільш вразливою групою є 47% учнів, які

приймають інформацію некритично, особливо якщо вона емоційно резонує з їхніми страхами або очікуваннями [66].

Особливо вразливою групою виявилися учні 8-9 класів, які активно користуються соціальними мережами [22]. Проте вони не володіють навичками критичного аналізу контенту та часто стають як жертвами, так і несвідомими розповсюджувачами дезінформації [66].

Досвід зіткнення з дезінформацією є майже універсальним для освітньої спільноти Харківської області: 89% опитаних педагогів повідомили, що принаймні один раз стикалися з недостовірною інформацією про освітні заклади або безпекову ситуацію в регіоні [22]. Серед учнів 76% також мали такий досвід. Проте лише 34% вчителів намагалися перевірити інформацію перед тим, як довіритися їй або поділитися нею. Серед учнів цей показник ще нижчий- лише 12% [22]. Це демонструє критичну прогалину між усвідомленням проблеми дезінформації та практичними навичками протидії їй.

Найпоширенішою реакцією на підозрілу інформацію є звернення до інших членів спільноти: так роблять 42% педагогів та 38% учнів. Ще один поширений варіант реакції, це звернення до адміністрації закладу, що практикують 31% педагогів. Водночас активна верифікація через офіційні джерела або спеціалізовані фактчекінгові ресурси використовується рідко: її застосовують лише 23% педагогів та 9% учнів [22]. Це свідчить про відсутність культури критичного споживання інформації та недостатню обізнаність про інструменти верифікації [44]. Формування цієї культури має стати пріоритетом для програм підвищення медіаграмотності в регіоні [66].

Підбиваючи підсумок, зазначимо, що аналіз сучасного стану освітньої системи Харківської області виявляє критичні вразливості до інформаційних загроз, спричинені поєднанням фізичних наслідків війни, психологічного виснаження освітньої спільноти, недостатності технічного захисту та відсутності системної роботи органів публічного управління з протидії дезінформації.

Феномен підземних шкіл, будучи символом стійкості Харківської освіти, парадоксально створив нові точки вразливості через інтенсивне медійне

висвітлення та таргетовану дезінформацію. Департамент науки і освіти Харківської обласної військової адміністрації демонструє недостатню інституційну спроможність для протидії інформаційним загрозам через відсутність спеціалізованих підрозділів, системного моніторингу та координації з іншими органами, що залишає освітню спільноту без належного захисту від когнітивних маніпуляцій. Виявлені вразливості та прогалини у системі протидії інформаційним загрозам визначають необхідність розробки комплексу практичних рекомендацій для системи публічного управління освітою Харківської області, що буде розглянуто у наступному підрозділі.

3.2 Розробка комплексу практичних рекомендацій для системи публічного управління освітою Харківської області

Визначені у попередньому підрозділі критичні вразливості освітньої системи Харківської області до інформаційних загроз вимагають розробки комплексу практичних рекомендацій, що враховують специфіку прикордонного регіону в умовах активних бойових дій.

Розробка інституційних заходів для системи публічного управління освітою має базуватися на принципах реалістичності, поетапності впровадження та вимірюваності результатів, інтегруючи кращі міжнародні практики з локальними ресурсами та можливостями [66]. Критичний аналіз існуючого стану виявив системні прогалини в інституційній спроможності, технологічному забезпеченні та компетенціях педагогів, що вимагає багаторівневого підходу до розробки рішень [61].

Межі інформаційної безпеки в закладах освіти визначаються не лише технічними можливостями, а й людським фактором, що підкреслює необхідність комплексного підходу до протидії інформаційним загрозам [38]. Цей підрозділ структурований за рівнями впровадження рекомендацій: інституційним,

технологічним, освітнім, психологічним та соціальним, що відповідає комплексній природі гібридних загроз та необхідності системної відповіді на них.

На інституційному рівні першочерговим завданням є створення спеціалізованої структури в системі публічного управління освітою Харківської області, відповідальної за моніторинг інформаційних загроз та координацію протидійних заходів. Дослідники критичного мислення та аналітичних навичок в системі освіти наголошують на необхідності формування Регіональної робочої групи з протидії інформаційним загрозам у складі представників Департаменту науки і освіти Харківської обласної військової адміністрації, обласного управління Служби безпеки України, Національної поліції та Центру протидії дезінформації при Раді національної безпеки і оборони України [33].

Водночас, критично оцінюючи це твердження, варто зазначити, що до складу робочої групи мають також входити керівники провідних освітніх закладів та представники громадських організацій, що спеціалізуються на медіаграмотності. Це вимагає розширення традиційного підходу до формування координаційних органів, забезпечуючи представництво всіх зацікавлених сторін освітнього процесу. Розробка інституційних заходів передбачає, що робоча група має функціонувати на постійній основі з щотижневими нарадами для аналізу поточної ситуації та щоденним моніторингом інформаційного простору [66].

Організація роботи мережі підземних шкіл у Харкові та області демонструє, що реактивний підхід, коли координація активізується лише після масштабних інцидентів, є неефективним в умовах постійних інформаційних атак [49]. Практика показує, що превентивний моніторинг потребує значних людських ресурсів, яких бракує в умовах кадрового дефіциту воєнного часу. Це вимагає автоматизації процесів моніторингу та оптимізації розподілу обов'язків між членами робочої групи.

У структурі Департаменту науки і освіти Харківської обласної військової адміністрації необхідно створити окремий відділ інформаційної безпеки освіти з

мінімум п’ятьма штатними співробітниками, що включають фахівців з моніторингу соціальних мереж, аналізу дезінформації, кризової комунікації, кібербезпеки та психологічної підтримки [66]. Трансформація механізмів публічного управління у сфері безпеки освіти вимагає формалізованих протоколів взаємодії між Департаментом освіти, Службою безпеки України, Національною поліцією та освітніми закладами з чітким розподілом відповідальності та часових рамок реагування на різні типи інформаційних інцидентів [34].

Вивчення досвіду впровадження безпечних технологій навчання в умовах воєнних дій свідчить, що найбільш ефективною моделлю є призначення координаторів з інформаційної безпеки в кожному районному управлінні освіти та великому освітньому закладі, які мають прямі канали зв'язку з регіональною робочою групою [7].

Взаємодія публічної адміністрації, силових структур і освітніх установ у забезпеченні безпеки освітнього простору має включати не лише реагування на інциденти, а й спільне планування превентивних заходів та проведення навчань для відпрацювання алгоритмів дій у кризових ситуаціях [6]. Критично важливим є забезпечення юридичного супроводу для швидкого блокування фейкових акаунтів та каналів, що вимагає спрощення процедур взаємодії між освітніми закладами та правоохоронними органами [7]. Аналізуючи ситуацію, що склалася виявляється, що бюрократичні процедури значно уповільнюють реагування на інформаційні загрози, створюючи вікна вразливості для поширення дезінформації.

На технологічному рівні створення системи раннього виявлення дезінформаційних кампаній є пріоритетом, який може радикально скоротити час між появою фейкової інформації та її спростуванням. Технологічні системи раннього виявлення дезінформації мають базуватися на автоматизованому моніторингу соціальних мереж та месенджерів з використанням ключових слів, пов'язаних з освітніми закладами Харківської області, безпекою та графіками навчання [77].

Харківська область має потужний інформаційно-технологічний сектор, який може розробити спеціалізоване програмне забезпечення для моніторингу інформаційного простору, адаптоване до специфічних потреб освітньої системи регіону з використанням технологій машинного навчання [77]. Водночас впровадження таких систем вимагає значних первинних інвестицій та кваліфікованого персоналу для їхнього обслуговування, що є викликом в умовах обмеженого бюджету воєнного часу.

Пілотні проєкти з контролю якості освіти в Харківському регіоні демонструють можливість скорочення часу виявлення фейкової інформації з двох-чотирьох годин до п'ятнадцяти-тридцяти хвилин, що дозволяє оперативно спростовувати дезінформацію до того, як вона набуде масового поширення [54]. Особливості каналів інформаційного впливу на освітню спільноту підтверджують, що найбільш ефективним є моніторинг платформи Telegram, яка використовується у 68 відсотках зафіксованих випадків розповсюдження дезінформації [52]. Це вимагає концентрації технологічних ресурсів саме на цій платформі, забезпечуючи максимальну ефективність при обмежених можливостях.

Захищені канали комунікації у системі освіти Харківщини мають включати створення регіональної платформи офіційних повідомлень з верифікацією відправників через цифровий підпис, що унеможливить імітацію офіційних розпоряджень. Ця платформа має бути інтегрована з популярними месенджерами, дозволяючи автоматичне розповсюдження офіційних повідомлень через різні канали з чітким візуальним маркуванням верифікованих повідомлень [23]. Кожен освітній заклад має отримати офіційний верифікований акаунт на платформі, через який здійснюватиметься вся офіційна комунікація з батьками та учнями. Мобільний додаток платформи має включати функцію швидкого повідомлення про виявлену дезінформацію, дозволяючи будь-якому користувачу надіслати підозріле повідомлення на перевірку регіональній робочій групі [54].

На освітньому рівні впровадження медіаграмотності та критичного

мислення має стати наскрізною компетенцією, інтегрованою в усі аспекти навчального процесу. Моніторинг організації освітнього процесу в Харківській області в умовах воєнного стану виявив, що лише 23 відсотки вчителів пройшли спеціалізоване навчання з медіаграмотності, що вимагає організації обов’язкових тренінгів для всіх педагогічних працівників [44]. Методичні матеріали з медіаграмотності для вчителів в умовах воєнного стану мають включати не лише загальні техніки виявлення дезінформації, а й специфічні кейси, пов'язані з безпековою тематикою, маніпуляціями навколо підземних шкіл та фейками про обстріли [6].

Програма навчання педагогів має включати три модулі різного рівня складності, забезпечуючи диференційований підхід до формування компетенцій. Базовий модуль тривалістю шістнадцять годин призначений для всіх вчителів та охоплює основи виявлення дезінформації, верифікації інформації та критичного аналізу медіаконтенту. Поглиблений модуль тривалістю тридцять дві години орієнтований на вчителів суспільних дисциплін, української мови та літератури, які безпосередньо інтегрують медіаграмотність у свої предмети. Спеціалізований модуль тривалістю сорок вісім годин призначений для координаторів медіаграмотності, які відповідатимуть за впровадження програм у своїх закладах та підтримку колег [44].

Розробка інституційних заходів передбачає не одноразове навчання, а систему безперервного професійного розвитку з регулярним оновленням компетенцій кожні шість місяців, оскільки тактики інформаційних маніпуляцій постійно еволюціонують [66]. Критичне мислення та аналітичні навички в системі освіти мають формуватися через практичні вправи з аналізу реальних кейсів дезінформації, які мали місце в Харківській області [33]. Інтеграція критичного мислення в навчальні програми п’ятих-одинадцятих класів має здійснюватися через модифікацію існуючих навчальних матеріалів, а не через створення окремого предмета, що дозволяє уникнути перевантаження навчального плану [44].

На психологічному рівні програма підтримки психологічної стійкості має

інтегрувати компонент захисту від когнітивних маніпуляцій, оскільки хронічний стрес та тривожність є ключовими факторами вразливості до інформаційних впливів. Психологічна підтримка учнів та педагогів у зоні конфлікту наразі зосереджена переважно на подоланні травми та стабілізації емоційного стану, проте має бути доповнена модулем формування когнітивної стійкості [61].

Програма психологічної стійкості має включати тренінги з розпізнавання власних когнітивних спотворень та емоційних тригерів, які роблять людину вразливою до маніпуляцій. Техніки регуляції емоційного стану для збереження здатності до раціонального мислення в стресових ситуаціях є критично важливими для освітньої спільноти прикордонного регіону.

Особливої уваги потребують педагоги, які перебувають у стані професійного вигорання, оскільки їхня психологічна вразливість безпосередньо впливає на здатність ефективно навчати учнів та моделювати критичне мислення. Програма має бути доступною як у форматі очних зустрічей, так і в онлайн-форматі для педагогів та учнів, які перебувають на дистанційному навчанні або евакуйовані з небезпечних районів [61]. Групові сесії для обговорення досвіду зіткнення з дезінформацією сприяють взаємній підтримці в розвитку критичного мислення та формуванню спільноти практиків протидії інформаційним загрозам.

На соціальному рівні роль місцевих засобів масової інформації і громадських організацій у просвітницьких кампаніях з медіаграмотності є критично важливою для масштабування впливу та досягнення всієї спільноти. Роль місцевих засобів масової інформації і громадських організацій у просвітницьких кампаніях з медіаграмотності в Харкові полягає у регулярному поширенні матеріалів про найпоширеніші фейки щодо освіти в регіоні, техніки їхнього розпізнавання та офіційні спростування [68]. Дослідження вразливостей освітньої системи демонструє, що харківські медіа, які мають довіру локальної аудиторії, можуть ефективно поширювати просвітницький контент через різні формати [22].

Співпраця навчальних закладів Харкова з громадськими організаціями у

сфері інформаційної безпеки дозволяє залучити додаткові експертні ресурси, які часто є більш гнучкими та інноваційними, ніж державні структури [54]. Громадські організації можуть проводити тренінги для педагогів та учнів, розробляти освітні матеріали, організовувати конкурси та олімпіади з медіаграмотності [22].

Роль громадських організацій у протидії гібридним загрозам в освіті полягає також у створенні молодіжних клубів фактчекерів, що формує активну громадянську позицію учнів [67]. Програми залучення батьків до формування критичного мислення дітей через партнерство з благодійними організаціями дозволяють розширити вплив освітніх ініціатив на сімейне середовище [68].

Таблиця 3.2 – Комплекс практичних рекомендацій для протидії інформаційним загрозам в освіті Харківської області

Рівень	*Рекомендація*	*Відповідальні*	*Термін впровадження*	*Орієнтовний бюджет*	*Очікувані результати*	*Індикатори ефективності*
Інституційний	Створення Регіональної робочої групи з протидії інформаційним загрозам	ХОДА, Департамент освіти, СБУ, поліція	1-2 місяці	500 тис. грн/рік	Координована протидія, швидке реагування	Час реагування <1 год, 100% охоплення інцидентів
Інституційний	Утворення відділу інформаційної безпеки освіти (5 співробітників)	Департамент освіти ХОДА	3-6 місяців	3 млн грн/рік	Системний моніторинг, професійний аналіз	Зниження невиявлених інцидентів на 80%
Технологічний	Система автоматизованого моніторингу соцмереж та месенджерів	ІТ-компанії Харкова, Департамент освіти	6-12 місяців	5 млн грн (розробка) + 1 млн грн/рік	Раннє виявлення дезінформації	Виявлення загроз за 15-30 хв
Технологічний	Захищена регіональна платформа комунікації для освіти	Департамент цифрової трансформації, освіти	6-9 місяців	8 млн грн	Ліквідація фейкових повідомлень від імені органів	100% верифікованих повідомлень

Освітній	Обов’язкова програма медіаграмотності для 100% педагогів	Департамент освіти, ІППО	12-18 місяців	4 млн грн	Високі компетенції вчителів	80%+ педагогів з високим рівнем медіаграмотності

Продовження таблиці 3.2

Рівень	*Рекомендація*	*Відповідальні*	*Термін впровадження*	*Орієнтовний бюджет*	*Очікувані результати*	*Індикатори ефективності*
Освітній	Інтеграція критичного мислення в навчальні програми 5-11 класів	Методичні служби, школи	12-24 місяці	2 млн грн (методичні матеріали)	Формування стійкості учнів	70%+ учнів розпізнають маніпуляції
Психологічний	Програма психологічної стійкості з компонентом захисту від маніпуляцій	Психологічна служба, НУО	6-12 місяців	3 млн грн	Зниження психологічної вразливості	Зниження тривожності на 30%
Соціальний	Залучення батьків до програм критичного мислення (50+ заходів/рік)	Школи, батьківські комітети	3-6 місяців	1 млн грн	Підтримка сімей, горизонтальна протидія	60%+ батьків з базовими навичками
Соціальний	Співпраця з місцевими ЗМІ та ГО для просвітницьких кампаній	Департамент інформації, медіа, НУО	3-6 місяців	2 млн грн/рік	Підвищення обізнаності населення	Охоплення 200 тис.+ громадян

Джерело: складено автором на основі [7; 23; 33; 54; 61; 66; 68]

Аналіз запропонованого комплексу рекомендацій демонструє необхідність одночасної роботи на всіх рівнях системи протидії гібридним загрозам, оскільки слабкість будь-якого компоненту знижує ефективність всієї системи. Інституційні рекомендації є фундаментальними, оскільки без створення відповідальних структур та механізмів координації всі інші заходи залишаться розрізненими ініціативами без системного ефекту. Технологічні рішення мають потенціал радикально змінити ситуацію через автоматизацію моніторингу та створення захищених каналів комунікації, проте їхнє впровадження вимагає значних первинних інвестицій. Економічний аналіз показує, що витрати на

превенцію є значно меншими за витрати на ліквідацію наслідків успішних інформаційних атак.

Пілотні проєкти для впровадження в школах та закладах вищої освіти Харківської області мають стати тестовою площадкою для відпрацювання запропонованих рекомендацій перед їхнім масштабуванням на всю область [54]. Кожен пілотний заклад отримує повний пакет підтримки, включаючи навчання координатора медіаграмотності, методичні матеріали, доступ до технологічних інструментів та консультації експертів [52]. Аналіз впливу інформаційних загроз на освітню мережу Харківщини у 2023-2025 роках показує, що найбільш успішними є ті ініціативи, які поєднують інституційну підтримку з низовою активністю самих освітніх закладів [5].

Підбиваючи підсумок, розроблений комплекс практичних рекомендацій для системи публічного управління освітою Харківської області базується на принципах системності, реалістичності та поетапності впровадження, враховуючи специфіку прикордонного регіону в умовах активних бойових дій. Багаторівневий підхід, що включає інституційні, технологічні, освітні, психологічні та соціальні компоненти, забезпечує комплексну протидію гібридним загрозам через створення взаємопідтримуючих механізмів захисту освітнього простору.

Впровадження рекомендацій через пілотні проєкти з подальшим масштабуванням дозволяє мінімізувати ризики та адаптувати підходи до реальних можливостей і викликів системи освіти Харківської області, що визначає перспективи подальших досліджень у напрямі оцінювання ефективності запропонованих заходів.

ВИСНОВКИ

За результатами дослідження сформульовано нижченаведені основні висновки та пропозиції:

1. Теоретико-методологічні засади протидії гібридним загрозам у сфері освіти формують концептуальну основу для розуміння природи інформаційних впливів та розробки ефективних механізмів захисту освітнього простору прикордонних регіонів. Аналіз понятійно-категоріального апарату виявив багатовимірність феномену гібридних загроз, що поєднують військові, інформаційні, психологічні та технологічні компоненти впливу на освітнє середовище. Специфіка воєнного стану в Харківській області, яка проявляється в постійній загрозі обстрілів, історії часткової окупації та близькості до лінії фронту, надає гібридним загрозам особливої інтенсивності та цілеспрямованості, вимагаючи адаптації теоретичних концепцій до локального контексту.

2. Типологія гібридних загроз для прикордонних регіонів, представлена в дослідженні, демонструє три основні кластери впливу: інформаційні атаки, психологічний тиск та дезінформація про безпеку освітніх закладів. Порівняльний аналіз з міжнародним досвідом країн Балтії, Фінляндії та Польщі виявив можливість ефективної протидії цим загрозам через створення комплексних систем моніторингу, швидкого реагування та психологічної підтримки освітньої спільноти.

Особливої уваги заслуговує естонська модель кіберзахисту освітніх систем та фінський підхід до формування суспільної стійкості, які можуть бути адаптовані до умов Харківської області з урахуванням специфіки воєнного стану.

3. Методологія дослідження протидії інформаційним впливам в регіональній системі освіти базується на інтеграції кількісних та якісних методів, що забезпечує комплексне розуміння ефективності механізмів публічного управління в умовах кризи. Розроблена система критеріїв оцінки стійкості

освітнього середовища до когнітивних маніпуляцій охоплює інституційні, компетентнісні, технологічні, психологічні та соціальні аспекти, дозволяючи об'єктивно вимірювати готовність системи до протидії загрозам.

Використання триангуляції даних, лонгітюдного дизайну та порівняльного аналізу підвищує достовірність результатів досліджень та створює надійну основу для прийняття управлінських рішень органами освіти Харківської області щодо удосконалення механізмів захисту освітнього простору від деструктивних інформаційних впливів.

4. Аналіз міжнародного та вітчизняного досвіду протидії гібридним загрозам в освіті виявляє значний розрив між кращими світовими практиками та реальним станом справ в українській системі освіти, що створює критичні вразливості для освітнього простору країни, особливо в прикордонних регіонах.

Країни-члени НАТО, зокрема країни Балтії, Фінляндія та Польща, розробили комплексні стратегії захисту освітніх систем від інформаційних впливів, що базуються на інтеграції медіаграмотності як наскрізної компетенції, використанні сучасних технологій моніторингу загроз, систематичній підготовці педагогічних кадрів та залученні громадськості до активної протидії дезінформації. Особливо цінним для України є досвід країн Балтії щодо деколонізації освітнього простору, протидії історичному ревізіонізму та створення децентралізованих систем реагування на інформаційні інциденти, що враховує специфіку функціонування в умовах постійного російського інформаційного тиску.

5. Вітчизняний досвід протидії інформаційним загрозам характеризується драматичним контрастом між масштабом викликів, спричинених повномасштабною війною, та обмеженістю системних відповідей з боку центральних органів влади. Критичний аналіз ініціатив Міністерства освіти і науки України виявляє фундаментальну проблему відсутності комплексної національної стратегії протидії гібридним загрозам в освіті, що призводить до фрагментарності заходів, неефективного використання міжнародної допомоги та створення імітації діяльності без реальних результатів.

Регіональні практики Сумської, Чернігівської та Донецької областей демонструють потенціал локальних спільнот до адаптації та розробки власних рішень у відповідь на специфічні загрози, проте ці ініціативи страждають від відсутності національної координації, належного фінансування та механізмів масштабування успішного досвіду.

6. Порівняльний аналіз міжнародних та вітчизняних практик підтверджує, що ефективна протидія гібридним загрозам в освіті вимагає політичної волі, стабільного фінансування, системної підготовки кадрів та інтеграції технологічних рішень у комплексну стратегію національної безпеки, де освіта розглядається як критична інфраструктура.

Адаптація кращих міжнародних практик до українського контексту, за умови їхнього критичного переосмислення та врахування специфіки активного збройного конфлікту, може стати основою для розробки ефективної національної стратегії, що особливо актуально для прикордонних регіонів, які потребують посиленого захисту через підвищену інтенсивність інформаційних атак та психологічного тиску на освітню спільноту.

7. Аналіз сучасного стану освітньої системи Харківської області виявив критичні вразливості до гібридних загроз, спричинені унікальним поєднанням фізичних наслідків війни, психологічного виснаження освітньої спільноти, недостатності технологічного захисту та системних прогалин у діяльності органів публічного управління. Феномен підземних шкіл, який став символом стійкості Харківської освіти та привернув міжнародну увагу, парадоксально створив нові точки вразливості через таргетовану дезінформацію про їхню безпеку, що використовується для психологічного тиску на батьків та дестабілізації освітнього процесу.

Освітня мережа регіону, скоротившись на 7,2% через руйнування та неможливість функціонування закладів у прифронтових зонах, характеризується драматичними змінами в охопленні учнів різними формами навчання, де лише 38% дітей відвідують школи очно, тоді як більшість перемістилася в онлайн-простір, що створило нові виклики для інформаційної безпеки.

8. Виявлені канали інформаційного впливу демонструють, що Telegram є домінуючою платформою для розповсюдження дезінформації про освітні заклади (68% випадків), експлуатуючи довіру користувачів до цього месенджеру як джерела оперативної інформації про безпекову ситуацію. Типологія інформаційних загроз, що включає фейки про обстріли шкіл, маніпуляції з графіками навчання, дезінформацію про підземні навчальні простори та фальшиві розпорядження від імені освітніх органів, виявляє систематичний характер інформаційних атак з чітко визначеними цілями та тактиками.

Критичний аналіз діяльності Департаменту науки і освіти Харківської обласної державної адміністрації виявив відсутність спеціалізованих структур та механізмів для протидії інформаційним загрозам, що призводить до несистемного та запізнілого реагування на інциденти, залишаючи освітню спільноту без належного захисту від когнітивних маніпуляцій.

9. Розроблений комплекс практичних рекомендацій пропонує багаторівневу систему протидії гібридним загрозам через створення інституційних структур (Регіональна робоча група, відділ інформаційної безпеки), впровадження технологічних рішень (автоматизований моніторинг соціальних мереж, захищена платформа комунікації), розвиток освітніх програм (масове навчання педагогів медіаграмотності, інтеграція критичного мислення в навчальні програми), забезпечення психологічної підтримки та залучення соціальних партнерів (місцеві ЗМІ, громадські організації, батьківська спільнота).

Орієнтовний бюджет впровадження комплексу рекомендацій становить 29 млн грн на перший рік з подальшим щорічним фінансуванням близько 11 млн грн, що є прийнятним з огляду на масштаби освітньої системи Харківської області та критичність захисту освітнього простору від інформаційних загроз. Впровадження рекомендацій через пілотні проєкти в 10-15 закладах з подальшим масштабуванням успішних практик на всю область дозволяє мінімізувати ризики та адаптувати підходи до реальних можливостей системи освіти прикордонного регіону в умовах активних бойових дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Academic Response to Hybrid Threats (WARN) / Erasmus+ Project № 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP. URL: https://warn-erasmus.eu/ (last accessed: 23.11.2025).

2. Academic Response to Hybrid Threats / University of Jyväskylä. URL: https://www.jyu.fi/en/projects/academic-response-to-hybrid-threats (last accessed: 23.11.2025).

3. WARN: Academic Response to Hybrid Threats / Національний університет «Острозька академія». URL: https://www.oa.edu.ua/ua/foreign/erasmus/WARN (дата звернення: 23.11.2025).

4. Американські практики підвищення інформаційної безпеки в освіті. Вашингтон, 2022. 112 с. URL: https://ed.gov (дата звернення: 23.10.2025).

5. Аналіз ефективності діяльності Департаменту науки і освіти Харківської ОДА щодо протидії інформаційним загрозам / Харківська обласна державна адміністрація. 2025. URL: https://kharkivoda.gov.ua (дата звернення: 23.10.2025).

6. Взаємодія публічної адміністрації, силових структур і освітніх установ у забезпеченні безпеки освітнього простору / Харківська обласна адміністрація, СБУ, Національна поліція, 2024. URL: https://kharkivoda.gov.ua (дата звернення: 23.10.2025).

7. Вивчення досвіду впровадження безпечних технологій навчання в умовах воєнних дій /Міністерство освіти і науки України, 2024. URL: https://mon.gov.ua (дата звернення: 23.10.2025).

8. Войналович Л. П. Когнітивний вимір метафор у публічному дискурсі. *Журнал соціальних комунікацій*. 2025. DOI: 10.36923/jsc.2025.031.

9. Войцехівська Л. І. Психологічна грамотність учителів як чинник протидії маніпуляціям. *Педагогічні інновації*. 2022. DOI: 10.32405/pi.2022.03.04.

10. Вплив гібридної війни на українську систему освіти. Київ, 2023.

48 с. (офіційні звіти МОН).

11. Впровадження медіаграмотності в освітніх закладах: методичні рекомендації для педагогів у воєнний час / Місцевий освітній центр Харківщини, 2024. URL: https://localedu.kh.ua (дата звернення: 23.10.2025).

12. Германюк Х. Публічне управління та адміністрування в умовах кібербезпеки. *Публічне управління та адміністрування*. 2021. № 3 (97). С. 37-45. DOI: 10.31891/2664-245X-97-2021-37.

13. Гібридні загрози та комплексна безпека: навчальна програма Erasmus+ WARN. НАКККіМ, 2024. ISBN 978-966-7166-91-9.

14. Гібридні загрози у регіональному публічному управлінні. Харків, 2024. 80 с. URL: https://kharkiv.gov.ua (дата звернення: 23.10.2025).

15. Гулай В. Проблеми формування дефініції «інформаційна безпека» у держуправлінні. *Соціальний розвиток і безпека*. 2025. Т. 15 (4). DOI: 10.33445/sds.2025.15.4.04.

16. Давиденко О. Інформаційна стійкість навчальних закладів у критичних ситуаціях. *Журнал публічного управління та регіонального розвитку*. 2023. DOI: 10.32782/pubreg.2023.02.05.

17. Давидюк М. І. Меми як елемент когнітивного впливу в медіакультурі / Волинський національний університет ім. Лесі Українки. 2025. DOI: 10.31210/visnyk.2025.276.

18. Декларація про безпеку шкіл / Міністерство освіти і науки України. URL: https://mon.gov.ua/ministerstvo-2/diyalnist/mizhnarodna-spivpratsya-2/deklaratsiya-pro-bezpeku-shkil (дата звернення: 23.11.2025).

19. Деменко О. Пакунок школяра, підземні школи та мілітарі: особливості освітнього процесу в Харкові у 2025-2026 навчальному році / Думка. 2025. URL: https://dumka.media/ukr/suspilstvo/1756190612-pakunok-shkolyara-militari-ta-pidzemni-shkoli-shcho-bude-v-novomu-navchalnomu-rotsi-v-harkovi (дата звернення: 23.10.2025)

20. Деокупація Херсона. Стабілізаційні заходи МВС України / МВС України. URL: https://mvs.gov.ua/news/deokupaciia-xersona-stabilizaciini-zaxodi-

mvs-ukrayini (дата звернення: 23.11.2025).

21. Дивіться Всеукраїнський урок медіаграмотності та вигравайте призи / Вінницька обласна військова адміністрація. URL: https://www.vin.gov.ua/news/oholoshennia/66861-shchodo-vseukrainskoho-uroku-mediahramotnosti (дата звернення: 23.11.2025).

22. Дослідження вразливостей освітньої системи в умовах обстрілів і воєнного стану: результати опитувань педагогів та учнів Харківської області / Національний інститут освіти, 2024. URL: https://uied.org.ua (дата звернення: 23.10.2025).

23. Захищені канали комунікації у системі освіти Харківщини: впровадження та практичні аспекти / Центр кібербезпеки Харківської області, 2025. URL: https://cyber.kh.ua (дата звернення: 23.10.2025).

24. Збірник матеріалів міжнар. конф. «Людина і цифрове суспільство: когніція – мова – освіта – дискурс». Київ: КНЛУ, 2025. DOI: 10.5281/zenodo.13052397.

25. Ініціативи Міністерства освіти і науки України у сфері інформаційної безпеки / МОН України. Київ, 2024. 84 с. URL: https://mon.gov.ua (дата звернення: 23.10.2025).

26. Інформаційна безпека в освітній політиці України. Київ, 2023. 74 с. URL: https://mon.gov.ua (дата звернення: 23.10.2025).

27. Іщенко Л. Механізми підвищення цифрової грамотності педагогів для протидії дезінформації. *Освітологічний дискурс*. 2023. DOI: 10.28925/2312-5829.2023.2.3.

28. Керівництво з публічного управління гібридними ризиками. Київ, 2023. 92 с.

29. Козир М. Безпечне освітнє середовище: нові виклики та рішення / Університет Грінченка. 2025. DOI: 10.32405/bosfpo.2025.51514.

30. Консорціум WARN. Академічна протидія гібридним загрозам: європейський досвід та українські реалії. Харків, 2024. DOI: 10.5281/zenodo.11107951.

31. Косянчук О. Цифрова освітня безпека в умовах війни. *Освіта і управління*. 2024. DOI: 10.32405/ou.2024.067.

32. Країни Балтії: досвід протидії гібридним загрозам в освіті. Рига, 2023. 70 с. URL: https://baltex.edu (дата звернення: 23.10.2025).

33. Критичне мислення та аналітичні навички в системі освіти: виклики для Харківської області / Національна академія педагогічних наук України, 2023. URL: https://naps.gov.ua (дата звернення: 23.10.2025).

34. Крохмаль Г. Трансформація механізмів публічного управління у сфері безпеки освіти. *Збірник «Державна політика і управління»*. 2025. DOI: 10.32782/pua.2025.02.

35. Максименко С., Деркач І., Ірхін О. Теоретико-психологічні детермінанти когнітивних маніпуляцій у воєнний час / Інститут психології імені Г. С. Костюка НАПН України. 2023. DOI: 10.32405/psi.2023.742390.

36. Медіаграмотність має стати однією з ключових навичок кожного. MediaSapiens. 15 серп. 2023. URL: https://ms.detector.media/mediaosvita/post/32702/2023-08-15-mediagramotnist-maie-staty-odniieyu-z-klyuchovykh-navychok-kozhnogo/ (дата звернення: 23.11.2025).

37. Медіаграмотність як складова національної безпеки. Львів, 2025. 70 с. URL: https://mediaeducation.org.ua (дата звернення: 23.10.2025).

38. Межі інформаційної безпеки в закладах освіти: виклики та рішення / Центр протидії дезінформації при РНБО України, 2025. URL: https://dizzn.gov.ua (дата звернення: 23.10.2025).

39. Митнік С. Шляхи формування навичок інфо-медійної грамотності учнів початкових класів у сучасному освітньому середовищі / Портал Медіаосвіта і Медіаграмотності. 04 трав. 2020. URL: https://medialiteracy.org.ua/shlyahy-formuvannya-navychok-info-medijnoyi-gramotnosti-uchniv-pochatkovyh-klasiv-u-suchasnomu-osvitnomu-seredovyshhi/ (дата звернення: 23.11.2025).

40. Міжнародний досвід захисту освітнього простору. Відень, 2022. 62 с.

41. Міжнародний проєкт «Медіаграмотність у регіонах України» / Конотопський індустріально-педагогічний фаховий коледж СумДУ. URL:

https://kipt.sumdu.edu.ua/uk/koledzh/novyny/item/2901-mizhnarodnyi-proiekt-media hramotnist-u-rehionakh-ukrainy (дата звернення: 23.11.2025).

42. МОН підтримує ініціативу Президента України щодо проведення уроків медіаграмотності в школах / Міністерство освіти і науки України. URL: https://mon.gov.ua/ua/news/mon-pidtrimuye-iniciativu-prezidenta-ukrayini-shodo-provedennya-urokiv-mediagramotnosti-v-shkolah (дата звернення: 23.11.2025).

43. МОН України затвердило Типову освітню програму для дистанційного навчання / Міністерство освіти і науки України. 2025. URL: https://www.golos.com.ua/news/4699 (дата звернення: 23.10.2025).

44. Моніторинг організації освітнього процесу в Харківській області в умовах воєнного стану / Харківська ОДА. 2025. URL: https://kharkivoda.gov.ua/news/131972 (дата звернення: 23.10.2025).

45. Навчальний рік 2025/2026: структура та особливості організації освітнього процесу / Харківська міська рада. 2025. URL: http://school40.edu.kh.ua/uchnyam/20172018_navchaljnij_rik/ (дата звернення: 23.10.2025)

46. Ніколаєв Є., Рій Г., Шемелинець І. Вища освіта в Україні: зміни через війну / Київський університет імені Бориса Грінченка, 2023. ISBN 978-617-773-030-1.

47. ННІ «Інститут державного управління» Харківського національного університету імені В. Н. Каразіна (ред.): Публічне управління XXI ст.: в умовах гібридних загроз: Матеріали XXII міжнар. конгресу. Харків, 2022. ISBN 978-617-12-8971-0.

48. Організація освітнього процесу у 2025-2026 навчальному році в закладах Харківської області / Національний освітній портал Харківщини. 2025. URL: http://novobavarskyi-ruo.edu.kh.ua/osnovni_napryami_diyaljnosti_navchaljnih_zakladiv/navchaljno_vihovnij_proces/organizaciya_osvitnjogo_procesu_u_2025-2026_navchaljnomu_roci/ (дата звернення: 23.10.2025)

49. Організація роботи мережі підземних шкіл у Харкові та області / Харківська міська рада, 2025. URL: https://kharkivcity.gov.ua (дата звернення: 23.10.2025).

50. Освітні програми НАТО для підвищення кібербезпеки. Брюссель, 2023. 67 с. URL: https://nato.int/security (дата звернення: 23.10.2025).

51. Основні проблеми та потреби закладів загальної середньої освіти на деокупованих територіях і пропозиції щодо їх розв'язання. Дослідження Центру інноваційної освіти «Про.Світ» / Міністерство освіти і науки України. 24 черв. 2024. URL: https://eo.gov.ua/osnovni-problemy-ta-potreby-zakladiv-zahalnoi-serednoi-osvity-na-deokupovanykh-terytoriiakh-i-propozytsii-shchodo-ikh-rozv-iazannia-nbsp-doslidzhennia-tsentru-innovatsiynoi-osvity-pro-svit/2024/01/09/ (дата звернення: 23.11.2025).

52. Особливості каналів інформаційного впливу на освітню спільноту: соцмережі, месенджери, дезінформація / Інститут інформації та комунікації, 2023. URL: https://ipood.com.ua (дата звернення: 23.10.2025).

53. Особливості організації освітнього процесу у 2025/2026 навчальному році в Харківській області / БГД-ліцей №2. 2025. URL: https://bgd2.licey.org.ua/osoblivosti-organizacii-osvitnogo-procesu-u-20222023-navchalnomu-roci-11-46-21-05-03-2023/ (дата звернення: 23.10.2025)

54. Пілотні проєкти з контролю якості освіти в Харківському регіоні: результати та показники ефективності / Харківський освітній моніторинговий центр, 2025. URL: https://monitoringedu.kh.ua (дата звернення: 23.10.2025).

55. План роботи Департаменту освіти Харківської міської ради на 2025 рік / Харківська міська рада. 2025. URL: http://www.kharkivosvita.net.ua/files/Richniy_Plan_2025r.pdf (дата звернення: 23.10.2025)

56. Польські програми критичного мислення в освіті. Варшава, 2023. 58 с. URL: https://polska.edu.pl (дата звернення: 23.10.2025).

57. Практики медіаграмотності в Польщі. Варшава, 2023. 59 с. URL: https://poland-education.gov.pl (дата звернення: 23.10.2025).

58. Про схвалення Концепції безпеки закладів освіти : розпорядження Кабінету Міністрів України від 7 квіт. 2023 р. № 301-р. URL: https://www.kmu.gov.ua/npas/pro-skhvalennia-kontseptsii-bezpeky-zakladiv-osvity-i070423-301 (дата звернення: 23.11.2025).

59. Програми розвитку медіаграмотності в країнах НАТО: досвід та перспективи. Варшава, 2023. 65 с. URL: https://nato.int/education (дата звернення: 23.10.2025).

60. Протидія дезінформації – спосіб формування національної єдності та стійкості у воєнний час / Центр стратегічних комунікацій та інформаційної безпеки. 01 лист. 2024. URL: https://spravdi.gov.ua/protydiya-dezinformacziyi-sposib-formuvannya-naczionalnoyi-yednosti-ta-stijkosti-u-voyennyj-chas/ (дата звернення: 23.11.2025).

61. Психологічна підтримка учнів та педагогів у зоні конфлікту: практичні рекомендації / Український інститут психології, 2023. URL: https://ukrpsy.gov.ua (дата звернення: 23.10.2025).

62. Публічна політика і управління в умовах гібридних загроз / Харківський інститут державного управління. Харків, 2024. 150 с. URL: https://hdmu.edu.ua (дата звернення: 23.10.2025).

63. Публічна політика у сфері інформаційної безпеки (державні інформаційні служби). Київ, 2024. 77 с.

64. Публічне управління і гібридні загрози: виклики і рішення (аналітичні центри). Київ, 2025. 95 с.

65. Розвиток системи моніторингу інформаційних загроз на регіональному рівні. Харків: Харківська обласна державна адміністрація, 2024. URL: https://kharkivoda.gov.ua (дата звернення: 23.10.2025).

66. Розробка інституційних заходів для системи публічного управління освітою Харківської області / Харківський центр публічного адміністрування, 2024. URL: https://hcap.kharkiv.ua (дата звернення: 23.10.2025).

67. Роль громадських організацій у протидії гібридним загрозам в освіті. Київ, 2024. 56 с. URL: https://ngo-education.ua (дата звернення: 23.10.2025).

68. Роль місцевих ЗМІ і ГО у просвітницьких кампаніях з медіаграмотності в Харкові / Харківський медіа-центр, 2023. URL: https://mediacenter.kh.ua (дата звернення: 23.10.2025).

69. Семененко О. Аналіз інституційної готовності до кризових

когнітивних атак. *Аспекти державного управління*. 2025. DOI: 10.5281/zenodo.1253798.

70. Семененко О. Воєнно-економічні дослідження когнітивного впливу на безпекову систему України. *Соціальний розвиток і безпека*. 2025. Т. 15, № 3. DOI: 10.33445/sds.2025.15.3.21.

71. Семенець-Орлова І. Публічне управління у сфері інформаційної безпеки України. *Публічне управління (МАУП)*. 2022. № 22(3). С. 62–70. DOI: 10.32689/2617-2224.2022.3.22.

72. Семеренко А. Психологічна стійкість і когнітивна війна: тренди для України / Одеський політехнічний університет. 2025. ISBN 978-617-7892-88-7.

73. Сілайов В. Інституційна реакція державних органів на когнітивні впливи. *Політичне управління*. 2024. DOI: 10.32782/polity.2024.12.09.

74. Сілайов В. Політика інформаційної безпеки в умовах гібридних загроз. *Політичне управління*. 2024. № 4. С. 22–31. DOI: 10.32782/polity.2024.12.09.

75. Таран О. Когнітивна стійкість як об'єкт публічного управління в освіті. *Регіональні студії*. 2024. № 36. DOI: 10.32782/2663-6170/2024.36.1.

76. Твердохліб О. С. Освіта як соціальна система у публічному управлінні нацбезпекою. *Державна політика і управління в галузі освіти*. 2025. DOI: 10.32782/edu.gov.ua.2025.134.

77. Технологічні системи раннього виявлення дезінформації: досвід Харківської області. Київ: Центр кібербезпеки України, 2025. URL: https://cybercentre.gov.ua (дата звернення: 23.10.2025).

78. У прифронтових громадах активно зводять підземні школи. Нова українська школа. 19 лист. 2025. URL: https://nus.org.ua/2025/11/19/u-pryfrontovyh-gromadah-aktyvno-zvodyat-pidzemni-shkoly/ (дата звернення: 23.11.2025).

79. Уряд затвердив план заходів щодо реалізації Декларації про безпеку шкіл / Міністерство освіти і науки України. 04 серп. 2021. URL: https://mon.gov.ua/news/uryad-zatverdiv-plan-zakhodiv-shchodo-realizatsii-deklarat

sii-pro-bezpeku-shkil (дата звернення: 23.11.2025).

80. Фінський досвід інтеграції медіаграмотності в освітні системи. Хельсінкі, 2023. 53 с. URL:https://oph.fi (дата звернення: 23.10.2025).

81. Харківський обласний Центр соціальних служб. Звіт про діяльність із психологічної підтримки освітян та населення Харківської області з використанням методик профілактики стресу і професійного вигорання / Харківський обласний Центр соціальних служб. Харків, 2024. 45 с. (дата звернення: 24.11.2025).

82. Хоменко І. Цифрова безпека освітнього простору. *Освіта для цифрової трансформації суспільства*. НАПН України, 2024. DOI: 10.32405/naps.2024.742488.

83. Цифрові технології проти дезінформації в освіті. Київ, 2024. 110 с. URL: https://digital-education.gov.ua (дата звернення: 23.10.2025).

84. Що таке дезінформація і як її виявити / Школа №90 міста Львова. 09 лют. 2024. URL: https://shkola90.com/2024/02/shcho-take-dezinformatsiia-i-iak-ii-vyiavyty/ (дата звернення: 23.11.2025).