ПРИКЛАДНІ СОЦІАЛЬНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК [070.4:004.738.5]:316.77]:355.02(477)"2022/2024"
DOI https://doi.org/10.32782/2710-4656/2025.5.2/54

Бистров А. Б.
Київський національний університет імені Тараса Шевченка

ТРАНСФОРМАЦІЯ КРИЗОВИХ КОМУНІКАЦІЙ УКРАЇНСЬКИХ ОНЛАЙН-МЕДІА ПІД ЧАС ВІЙНИ

Стаття присвячена комплексному аналізу трансформації кризових комунікацій українських онлайн-медіа в період повномасштабного вторгнення РФ (лютий 2022 р. – грудень 2024 р.). Актуальність дослідження зумовлена безпрецедентними викликами, що змусили медіа функціонувати в умовах «подвійної кризи»: з одного боку, протистояти зовнішній гібридній агресії Росії, а з іншого – реагувати на посилення внутрішнього тиску з боку вітчизняних політичних та силових акторів.

У статті розкрито основні форми та джерела тиску на українські медіа. На основі аналізу звітів моніторингових організацій (IMI, «Детектор медіа», RSF, CPJ, Freedom House), а також якісного аналізу резонансних кейсів тиску на редакції Bihus.Info та «Українська правда» досліджено та систематизовано загрози.

Визначено, що зовнішній тиск з боку РФ характеризується високою агресією і включає масовані кібератаки, фізичні злочини проти журналістів та руйнування медійної інфраструктури. Водночас розглянуто прояви внутрішнього тиску, який посилився і включає: політичне та адміністративне втручання (спроби впливу на редакційну політику, використання мобілізації як інструменту тиску), незаконне стеження та прослуховування, економічні утиски (тиск на рекламодавців) та юридичне переслідування.

У відповідь на ці виклики досліджено фундаментальну трансформацію алгоритмів кризової комунікації редакцій.

Обґрунтовано введення поняття «моделі проактивного кризового опору» – інноваційної стратегії, що виходить за межі класичних теорій (SCCT, IRT), які виявилися обмеженими в умовах гібридної війни.

З'ясовано, що застосування такої моделі перетворює кризову комунікацію з інструменту управління репутацією на форму активного опору та механізм забезпечення інституційної сталості й захисту свободи слова.

Доведено дієвість цих стратегій у мобілізації суспільної підтримки та здатності впливати на реакцію влади в окремих резонансних випадках, що призводило до відкриття кримінальних проваджень та кадрових рішень. Разом з тим зроблено висновок, що ці стратегії не вирішують системних проблем, зокрема критичної залежності від зовнішнього фінансування та загальної фінансової нестабільності редакцій, що залишається ключовою загрозою для їхньої операційної стійкості.

Ключові слова: *кризова комунікація, онлайн-медіа, гібридна війна, дезінформація, тиск на журналістів, свобода слова, подвійна криза, комунікація-опір, модель проактивного опору, медіастійкість.*

Постановка проблеми. Повномасштабне військове вторгнення Російської Федерації (РФ) в Україну 24 лютого 2022 року стало екзистенційним викликом для української державності та суспільства [1]. Ця збройна агресія радикально трансформувала не лише політичний, економічний та соціальний ландшафт країни, але й спричинила глибокі зміни в медіасфері та інформаційному просторі. Війна ведеться не лише на фізичному полі бою, а й в інформаційній площині. Там РФ розгорнула безпрецедентну за масштабами та інтенсивністю кампанію дезінформації, пропаганди та маніпуляцій, спрямовану на радикальний підрив української стійкості, деморалізацію сус-

пільства та дискредитацію української влади на міжнародній арені.

В умовах війни критично зросла роль онлайн-медіа та соціальних мереж як основних джерел новин для українців. Згідно з даними опитувань, проведених 2023 року, 77,9 відсотків громадян покладалися на соціальні медіа для отримання новин, а 70 відсотків використовували їх як першочергове джерело інформації. Українські медіа, особливо онлайн-платформи, взяли на себе критично важливу місію: інформування суспільства про перебіг бойових дій, документування воєнних злочинів РФ, підтримку національної єдності та протидію ворожій дезінформації [2; 3].

Після 24 лютого 2022 року українські редакції, передусім онлайн-медіа, зіткнулися з комплексом безпрецедентних викликів та загроз. Журналісти зазнають постійної фізичної небезпеки: фіксуються численні випадки вбивств, поранень, викрадень та незаконних затримань представників медіа російськими військовими та окупаційними адміністраціями [4]. Руйнування зазнає медійна інфраструктура, включно з офісами редакцій, радіоретрансляторами та телевежами [4; 5]. Постійним фактором тиску стали масовані кібератаки, спрямовані на виведення з ладу сайтів, викрадення даних та поширення фейків [6; 7; 8]. Війна спричинила глибоку економічну кризу в медіасекторі, призвівши до колапсу рекламного ринку та критичної залежності багатьох видань від зовнішнього фінансування, переважно грантової підтримки. Директорка Інституту масової інформації Оксана Романюк стверджує, що «практично 90% українських медіа виживали завдяки грантам» [9]. На додачу до зовнішніх загроз, пов'язаних з російською агресією, українські медіа стикаються і з внутрішнім тиском – політичним, адміністративним, юридичним та економічним, що походить від представників української влади, силових структур чи політичних опонентів [10; 11].

Такі екстремальні умови вимагають від редакцій онлайн-медіа не лише адаптації операційних процесів та моделей фінансування, але й кардинальної трансформації алгоритмів кризової комунікації. Під алгоритмами кризової комунікації в межах даної статті розуміється послідовність менеджерських дій, комунікаційних стратегій та протоколів, що застосовуються редакцією для ефективного реагування на різноманітні кризові ситуації.

Аналіз останніх досліджень і публікацій. Проблематика функціонування медіа в умовах війни та інформаційних загроз активно розробляється в працях українських науковців. Водночас світові дослідники, аналізуючи міжнародні конфлікти, фокусуються на ролі медіа у гібридних загрозах та механізмах захисту свободи слова. Звіти Інституту масової інформації (IMI), «Детектор медіа», Reporters Without Borders (RSF), Committee to Protect Journalists (CPJ) та Freedom House є важливими джерелами емпіричних даних для фіксації порушень прав журналістів [2; 7; 12; 13]. IMI системно документує випадки фізичних загроз та кібератак [14], а Державна служба спеціального зв'язку та захисту інформації України аналізує кіберзагрози з боку РФ [8]. Окремі кейси тиску, як-от стеження за командою Bihus.Info та тиск на «Українську правду», детально висвітлювалися в медіа та ставали предметом заяв професійних об'єднань, зокрема «Медіаруху» [10; 15; 16]. Досвід України є унікальним через поєднання повномасштабної військової агресії, кібервійни та внутрішньополітичного тиску, що зумовлює необхідність напрацювання нової теоретичної рамки.

Серед класичних підходів до вивчення кризових комунікацій найбільш релевантними є Теорія ситуаційної кризової комунікації (SCCT) [17] та Теорія відновлення іміджу (IRT) [18]. SCCT фокусується на тому, як організація має реагувати на кризу залежно від її типу та ступеня відповідальності. IRT зосереджується на риторичних стратегіях, які організація використовує для захисту свого іміджу.

Водночас досвід українських медіа демонструє обмеженість цих теорій. Розглянемо кейс тиску на редакцію Bihus.Info: згідно з SCCT та IRT, редакція як жертва мала б застосовувати стратегії мінімальної відповідальності або коригувальні дії. Частково це й було зроблено (відбулися кадрові зміни). Однак ключовим елементом реакції стало проведення власного розслідування та публікація доказів незаконного стеження з боку державних органів [15]. Ця проактивна контратака перетворила кризову комунікацію з інструменту захисту репутації на інструмент контр-тиску та боротьби за інституційну незалежність.

Цей та інші кейси свідчать про формування в українському медіапросторі нової моделі реагування, яку можна визначити як «Модель проактивного кризового опору». На відміну від класичних моделей, вона спрямована на захист свободи слова та забезпечення сталості діяльності медіа. Ключовими компонентами цієї моделі є: проактивна публічність, розслідувальна відповідь, мережева солідарність та міжнародна апеляція.

Попри значну кількість моніторингових даних, бракує комплексних наукових досліджень, які б систематизували форми тиску та, що найголовніше, аналізували б трансформацію саме алгоритмів кризової комунікації редакцій. Залишається недостатньо вивченим питання ефективності нових стратегій опору та їхньої відповідності класичним теоретичним моделям. Дана стаття спрямована на заповнення цієї лакуни.

Постановка завдання. Мета статті – виявлення характеру та джерел тиску на українські онлайн-медіа в період повномасштабного вторгнення РФ (лютий 2022 р. – грудень 2024 р.), з'ясування трансформацій у їхніх алгоритмах кризової комунікації, визначення ключових стратегій реагування та оцінка їхньої ефективності. Для досягнення мети сформульовано дослідницькі питання (ДП):

ДП1: Які основні форми та джерела тиску на українські онлайн-медіа спостерігалися у 2022–2024 рр.?

ДП2: Як трансформувалися алгоритми та стратегії кризової комунікації редакцій у відповідь на цей тиск?

ДП3: Наскільки ефективними були ці трансформовані стратегії?

ДП4: Як український досвід співвідноситься з класичними теоретичними моделями?

Дослідження охоплює період з лютого 2022 року по грудень 2024 року. Верхня хронологічна межа зумовлена необхідністю оперувати завершеними та верифікованими річними даними. На момент проведення дослідження повні та систематизовані дані за 2025 рік не є доступними, що могло б вплинути на об'єктивність аналізу темпоральних тенденцій.

Критерії відбору кейсів тиску: Для поглибленого якісного аналізу були обрані кейси тиску на редакції Bihus.Info та «Українська правда». Цей вибір зумовлений кількома факторами: по-перше, обидва інциденти мали значний суспільний резонанс та стали предметом широкого обговорення; по-друге, вони ілюструють широку палітру форм внутрішнього тиску – від незаконного стеження з боку спецслужб до політичного та економічного тиску з боку вищих органів влади; по-третє, редакції застосували розгорнуті та детально задокументовані у відкритих джерелах стратегії кризової комунікації, що дозволяє провести їхній глибокий аналіз.

Для формування вибірки кейсів використовувалися такі критерії:

– Інцидент стосувався українського онлайн-медіа (національного або регіонального рівня);

– Інцидент мав місце в період з лютого 2022 р. по грудень 2024 р.;

– Інцидент був задокументований у відкритих джерелах: звітах авторитетних міжнародних та українських моніторингових організацій (Інститут масової інформації (IMI), ГО «Детектор медіа» (ДМ), Reporters Without Borders (RSF), Committee to Protect Journalists (CPJ), Freedom House), офіційних звітах державних органів (Держспецзв'язку), публічних заявах самих медіа або в публікаціях інших незалежних та авторитетних медіа;

– Інцидент класифікується як форма тиску на медіа: кібератака, фізичний напад на журналістів/редакцію, політичний/адміністративний тиск, економічний тиск, юридичний тиск, кампанія з дезінформації або дискредитації.

Слід зауважити, що під час документування інцидентів тиску було обрано звіти IMI, «Детектор медіа», RSF, CPJ та Freedom House як організацій, що визнаються у міжнародній науковій та експертній спільноті як надійні джерела емпіричних даних щодо свободи медіа та безпеки журналістів. Їхні дані регулярно цитуються у наукових працях та використовуються у фахових звітах таких міжнародних інституцій, як ООН, Рада Європи та ОБСЄ, що підтверджує їхню валідність та авторитетність.

Методи збору даних: Аналіз документів: Проведено систематичний аналіз щорічних та періодичних звітів, моніторингів, заяв та пресрелізів міжнародних (RSF, CPJ, Freedom House, IPI) та українських (IMI, ДМ, «Медіарух») організацій.

Аналіз медіаконтенту: Здійснено аналіз публічних заяв, пресрелізів, редакційних колонок, постів у соціальних мережах та інших комунікаційних матеріалів, оприлюднених редакціями онлайн-медіа, що зазнали тиску.

Методи аналізу даних: Якісний аналіз кейсів: Застосовано для поглибленого вивчення найбільш резонансних та показових випадків тиску на медіа.

Контент-аналіз комунікаційних реакцій: Контент-аналіз комунікаційних реакцій застосовувався для систематизації стратегій, використаних медіа у відповідь на тиск. Аналізувались офіційні заяви редакцій, дописи у соціальних мережах, редакційні колонки та відеоматеріали (YouTube). Кодування здійснювалося за такими категоріями:

– Інформування: повідомлення про факт атаки/тиску;

– Атрибуція: вказування на ймовірне джерело атаки/тиску;

– Заклик до солідарності: звернення до медіаспільноти («Медіаруху»), громадських організацій та широкої аудиторії;

– Апеляція до влади: прямі публічні вимоги до правоохоронних органів та вищого керівництва держави розслідувати інцидент;

– Міжнародна апеляція: звернення до міжнародних правозахисних та журналістських організацій;

– Контр-розслідування: публікація власних розслідувань щодо інциденту;

Демонстрація стійкості: запевнення аудиторії у продовженні роботи попри тиск.

Тематичний аналіз звітів: Звіти моніторингових організацій аналізувалися для виявлення та систематизації основних тем і тенденцій.

Критерії оцінки ефективності кризових комунікацій:

– Збереження/відновлення довіри аудиторії;

– Операційна стійкість редакцій;

– Вплив на громадську думку та порядок денний;

– Відповідність заявленим цінностям/редакційним політикам.

Обмеження дослідження. Слід зазначити, що дане дослідження має певні обмеження. Відбір та аналіз кейсів тиску ґрунтується виключно на відкритих та задокументованих джерелах. Це не виключає існування випадків, що не отримали широкого публічного розголосу, особливо що стосується регіональних медіа або «м'яких»/латентних форм тиску, таких як самоцензура, «телефонне право», вибірковий допуск до брифінгів, позбавлення акредитації, тиск через податкові або рекламні механізми, що часто не документуються та не потрапляють до моніторингових звітів. Це обмежує повноту емпіричної бази й потребує подальших глибинних напівструктурованих інтерв'ю та внутрішніх кейсів з редакцій.

Виклад основного матеріалу. Для аналізу було відібрано та систематизовано 22 резонансні кейси тиску на українські онлайн-медіа/журналістів за період 2022–2024 рр., зібраних моніторинговими організаціями, зафіксованих у заявах самих медіа та задокументованих у відкритих джерелах.

Найбільш чисельною категорією є кібератаки (9 кейсів), також поширені політичний/адміністративний тиск (3 кейси), незаконне стеження (3 кейси) та юридичний тиск (3 кейси). Аналіз дозволяє виокремити дві основні категорії тиску: зовнішній, з боку РФ, та внутрішній, джерелами якого виступають українські державні інституції та інші внутрішні актори.

Зовнішній тиск з боку Російської Федерації характеризується високим рівнем агресії та спрямованістю на фізичне знищення або повне придушення українських медіа, а також на підрив довіри аудиторії до них. Він включає масовані кібератаки (DDoS, злами сайтів, фішинг) [19], кількість яких різко зросла після вторгнення. Відповідальність за них покладається на російські спецслужби та пов'язані з ними хакерські угруповання [20]. Також фіксуються численні фізичні злочини проти журналістів: вбивства, поранення, викрадення та руйнування технічної медійної інфраструктури [4; 5].

Поряд із зовнішньою агресією, незалежні медіа стикаються з тиском зсередини країни. Він проявляється у таких формах:

– Політичний та адміністративний тиск: зафіксовано спроби втручання в редакційну політику та можливе використання «темників» в агентстві «Укрінформ» [11; 19]; обмеження доступу до інформації та офіційних спікерів для незалежних медіа [10]; використання мобілізації як інструменту тиску на журналістів-розслідувачів [7; 19]; незаконне стеження та прослуховування, де найрезонанснішим став випадок зі стеженням СБУ за командою проєкту Bihus.Info [7; 15]. Про стеження також повідомляли журналісти Forbes Україна та «Української правди» [11].

– Економічний та юридичний тиск: редакція «Української правди» заявила про тиск з боку Офісу Президента на своїх рекламодавців [10]. Також спостерігається використання судових позовів проти журналістів та медіа [11; 21].

– Кампанії з дезінформації: анонімні Telegram-канали використовуються для системного переслідування та дискредитації незалежних медіа та моніторингових організацій [22].

Систематизація випадків та їх аналіз демонструють чіткий зв'язок між типом загрози та обраною стратегією реагування. У відповідь на кібератаки медіа застосовували переважно технічні заходи захисту, тоді як у відповідь на політичний тиск чи стеження редакції вдавалися до комплексних комунікаційних кампаній, задіюючи проактивну публічність, мережеву солідарність та міжнародну апеляцію. В умовах тиску редакції фундаментально трансформували свої підходи. У відповідь на внутрішній тиск українські медіа застосовували комплексні стратегії, які складаються у новий алгоритм реагування запропонованої «Моделі проактивного кризового опору»:

Проактивна публічність: Ця стратегія стала основним інструментом захисту. Кейс Bihus.Info, де редакція провела власне розслідування «Операція "Встид"» [15], та заява «Української правди» про тиск з боку Офісу Президента [10] є яскравими прикладами.

Мережева солідарність: Ключову роль відіграла потужна консолідація медіаспільноти через «Медіарух» [16];[23].

Розслідувальна відповідь: Використання журналістських розслідувань для викриття джерел тиску стало ефективною стратегією [11].

Апеляція до міжнародних стандартів: Звернення до CPJ, RSF, IPI та Єврокомісії стало важливим інструментом захисту [2; 7; 24].

Оцінка ефективності. Оцінка ефективності кризових комунікацій є комплексним завданням. Стратегія проактивної публічності та мережевої солідарності виявилася дієвою у приверненні уваги до проблеми тиску та спонуканні влади до реакції. Публікація розслідування Bihus.Info та широкий резонанс призвели до звільнення керівника Департаменту СБУ та відкриття кримінального провадження [15; 25]. Заяви «Української правди» викликали значну публічну дискусію та реакцію міжнародних організацій [26]. Водночас операційна стійкість медіа залишається під загрозою через колапс рекламного ринку та залежність від грантової підтримки [9], а щонайменше 216 медіа припинили роботу після вторгнення [12].

Висновки. Проведене дослідження дозволяє сформулювати низку висновків, що послідовно відповідають на поставлені дослідницькі питання (ДП).

Відповідь на ДП1 – У 2022–2024 рр. українські медіа опинились в ситуації, коли тиск надходить не лише від зовнішнього агресора (РФ), але й від внутрішніх акторів – представників виконавчої влади і силових структур. Зовнішній тиск з боку РФ проявлявся через масовані кібератаки [6; 7], фізичні злочини проти журналістів [4; 5] та дезінформаційні кампанії. Внутрішній тиск з боку українських акторів включав політичне втручання [10], незаконне стеження [15], економічні та юридичні утиски [10; 21]. Це створило унікальну ситуацію «подвійної кризи».

Відповідь на ДП2 – У відповідь на цей подвійний тиск відбулася фундаментальна трансформація алгоритмів кризової комунікації. У часи безпрецедентних викликів редакції перейшли від реактивних моделей управління репутацією до проактивних дій. Ключовими елементами нових стратегій стали максимальна публічність [15], мережева солідарність (зокрема, через «Медіарух») [16; 23], використання журналістських розслідувань як інструменту контр-тиску [15] та активна апеляція до міжнародної спільноти [24].

Відповідь на ДП3 – Трансформовані стратегії довели свою ефективність у мобілізації суспільної підтримки та здатності впливати на реакцію влади в окремих резонансних випадках [25]. Однак вони не вирішують системних проблем, таких як фінансова нестабільність редакцій [9] та збереження операційної стійкості [12].

Відповідь на ДП4 – Досвід України демонструє обмеженість класичних теорій кризової комунікації (SCCT, IRT) [17; 18], розроблених для умов мирного часу. Кризова комунікація для медіа в умовах гібридної війни перетворилася з інструменту управління репутацією на форму опору та механізм забезпечення сталості роботи редакцій, що ілюструє кейс Bihus.Info [15].

Таким чином, досвід українських онлайн-медіа в умовах повномасштабного вторгнення РФ доводить, що ефективна кризова комунікація сьогодні має виходити за межі реактивного захисту репутації. Вона стає інструментом активного захисту свободи слова, інституційної автономії та мобілізації суспільної підтримки. Запропонована модель проактивного кризового опору може стати основою для адаптації міжнародних теорій до реалій медіа країн, що перебувають у стані гібридної війни. Подальші дослідження можуть бути спрямовані на порівняльний аналіз стратегій реагування національних та регіональних медіа. Глибинний же аналіз трансформації кризових комунікацій українських онлайн-медіа набуває додаткової цінності при розгляді його у ширшому, міжнародному контексті функціонування медіа в умовах глобальних конфліктів та гібридних загроз. Стратегії, що напрацьовуються та апробовуються українськими медіа у «бойових» умовах, є не просто цінними уроками, а формують нову парадигму медіастійкості, що може бути адаптована та використана редакціями в інших країнах, які стикаються з гібридними загрозами.

Список літератури:

1. Повномасштабне військове вторгнення РФ в Україну. Вікіпедія: вільна енциклопедія. URL: https://en.wikipedia.org/wiki/Russian_invasion_of_Ukraine (дата звернення: 10.07.2025).

2. CPJ urges Ukraine president to halt media intimidation, allow journalists to work freely. Committee to Protect Journalists. 2024. URL: https://cpj.org/2024/12/cpj-urges-ukraine-president-to-halt-media-intimidation-allow-journalists-to-work-freely/ (дата звернення: 10.07.2025).

3. Ukraine: 1000 days on, journalists continue their fight. ARTICLE 19. 2024. URL: https://www.article19.org/resources/ukraine-1000-days-on-journalists-continue-their-fight/ (дата звернення: 10.07.2025).

4. Threats, attacks, destruction of newsrooms – how Russia targets Ukrainian media from frontline regions. Свідомі. 2025. URL: https://svidomi.in.ua/en/page/threats-attacks-destruction-of-newsrooms-how-russia-targets-ukrainian-media-from-frontline-regions (дата звернення: 10.07.2025).

5. ATTACKS ON MEDIA WORKERS IN UKRAINE IN 2024. Justice for Journalists Foundation. 2025. URL: https://jfj.fund/attacks-on-media-workers-in-ukraine-in-2024/ (дата звернення: 10.07.2025).

6. Росіяни за 3 роки з початку вторгнення здійснили щонайменше 100 кібератак на медіа і журналістів, – IMI. Детектор медіа. 2025. URL: https://ms.detector.media/withoutsection/post/37575/2025-02-21-rosiyany-za-3-roky-z-pochatku-vtorgnennya-zdiysnyly-shchonaymenshe-100-kiberatak-na-media-i-zhurnalistiv-imi/ (дата звернення: 10.07.2025).

7. Under attack: Press freedom three years since Russia's full-scale invasion of Ukraine. International Press Institute. 2025. URL: https://ipi.media/under-attack-press-freedom-three-years-since-russias-full-scale-invasion-of-ukraine/ (дата звернення: 10.07.2025).

8. Держспецзв'язку відзначає зменшення кібератак критичного рівня з боку РФ. Укрінформ. 2025. URL: https://www.ukrinform.ua/rubric-society/3958881-derzspeczvazok-vidznacae-zmensenna-kiberatak-kriticnogo-rivna-z-boku-rf.html (дата звернення: 10.07.2025).

9. Практично 90% українських медіа виживали завдяки грантам, – директорка Інституту масової інформації Оксана Романюк. Судово-юридична газета. 2024. URL: https://sud.ua/uk/news/publication/321895-prakticheski-90-ukrainskikh-media-vyzhivali-blagodarya-grantam-direktor-instituta-massovoy-informatsii-oksana-romanyuk (дата звернення: 10.07.2025).

10. «Українська правда» заявляє про системний тиск з боку Офісу Президента. Українська правда. 2024. URL: https://www.pravda.com.ua/columns/2024/10/9/7478844/ (дата звернення: 10.07.2025).

11. Як 2024 року українським журналістам перешкоджали працювати. MediaMaker. 2025. URL: https://mediamaker.me/news/tysk-pogrozy-napady-yak-2024-roku-ukrayinskym-zhurnalistam-pereshkodzhaly-praczyuvaty/ (дата звернення: 10.07.2025).

12. Attacks on journalists in Ukraine: 121 incidents in 2024 – report by the Justice for Journalists Foundation. National Union of Journalists of Ukraine. URL: https://nuju.org.ua/attacks-on-journalists-in-ukraine-121-incidents-in-2024-report-by-the-justice-for-journalists-foundation/ (дата звернення: 10.07.2025).

13. Ukraine: Freedom on the Net 2024 Country Report. Freedom House. 2024. URL: https://freedomhouse.org/country/ukraine/freedom-net/2024 (дата звернення: 10.07.2025).

14. IMI: щонайменше 127 випадків погроз та залякувань журналістів і медіа з боку Росії зафіксували з початку вторгнення. Детектор медіа. 2025. URL: https://detector.media/infospace/article/238448/2025-02-21-imi-shchonaymenshe-127-vypadkiv-pogroz-ta-zalyakuvan-zhurnalistiv-i-media-z-boku-rosii-zafiksuvaly-z-pochatku-vtorgnennya/ (дата звернення: 10.07.2025).

15. Бігус викрив СБУ на стеженні – відео, реакція, меми і деталі розслідування. NV. 2024. URL: https://nv.ua/ukr/ukraine/politics/bigus-vikriv-sbu-na-stezhenni-video-reakciya-memi-i-detali-rozsliduvannya-novini-ukrajini-50390285.html (дата звернення: 10.07.2025).

16. Медіарух закликав Зеленського негайно вжити заходів для припинення тиску на медіа з боку будь-яких держслужбовців. LB.ua. 2024. URL: https://lb.ua/culture/2024/10/10/639114_mediaruh_zaklikav_zelenskogo.html (дата звернення: 10.07.2025).

17. Coombs W. T. Ongoing crisis communication: Planning, managing, and responding. Sage publications, 2014.

18. Benoit W. L. Accounts, excuses, and apologies: A theory of image restoration strategies. Suny Press, 1995.

19. Барометр свободи слова за травень 2024 року. Інститут масової інформації. 2024. URL: https://imi.org.ua/monitorings/barometr-svobody-slova-za-traven-2024-roku-i61818 (дата звернення: 10.07.2025).

20. Список хакерських груп. Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Список_хакерських_груп (дата звернення: 10.07.2025).

21. У 2024 році суди переважно обмежувались умовними покараннями та штрафами за злочини проти журналістів – IMI. ZMINA.info. 2025. URL: https://zmina.info/news/u-2024-roczi-sudy-perevazhno-obmezhuvalysya-umovnymy-pokarannyamy-ta-shtrafamy-za-zlochyny-proty-zhurnalistiv-imi/ (дата звернення: 10.07.2025).

22. «ДМ» та IMI заявляють про організовану кампанію фейків і тиску з боку анонімних телеграм-каналів. Детектор медіа. 2023. URL: https://detector.media/infospace/article/219888/2023-11-28-dm-ta-imi-zayavlyayut-pro-organizovanu-kampaniyu-feykiv-i-tysku-z-boku-anonimnykh-telegram-kanaliv/ (дата звернення: 10.07.2025).

23. Учасники Медіаруху закликають президента припинити тиск на незалежні медіа з боку влади. Детектор медіа. 2024. URL: https://detector.media/infospace/article/233260/2024-10-10-uchasnyky-mediarukhu-zaklykayut-prezydenta-prypynyty-tysk-na-nezalezhni-media-z-boku-vlady/ (дата звернення: 10.07.2025).

24. Єврокомісія занепокоєна тиском на журналістів-розслідувачів в Україні, уряд закликали «діяти». Радіо Свобода. 2024. URL: https://www.radiosvoboda.org/a/news-yevrokomisiya-zhurnalisty-tysk-telemarafon/33180128.html (дата звернення: 10.07.2025).

25. У справі Bihus.Info відкрили нове кримінальне провадження про перешкоджання журналістській діяльності. Детектор медіа. 2024. URL: https://detector.media/infospace/article/222909/2024-02-13-u-spravi-bihusinfo-vidkryly-nove-kryminalne-provadzhennya-pro-pereshkodzhannya-zhurnalistskiy-diyalnosti/ (дата звернення: 10.07.2025).

26. Тиск на журналістів чи погана комунікація: що відбувається між ОП та «Українською правдою»? Радіо Свобода. 2024. URL: https://www.radiosvoboda.org/a/tysk-ukrayinska-pravda-ofis-prezydenta-shcho-vidomo/33153574.html (дата звернення: 10.07.2025).

Bystrov A. B. TRANSFORMATION OF CRISIS COMMUNICATIONS OF UKRAINIAN ONLINE MEDIA DURING THE WAR

The article is dedicated to a comprehensive analysis of the transformation of crisis communications of Ukrainian online media during the full-scale invasion by the Russian Federation (February 2022 – December 2024). The relevance of the study is driven by the unprecedented challenges that have forced the media to operate in a "dual crisis": on the one hand, countering Russia's external hybrid aggression, and on the other, responding to intensified internal pressure from domestic political and security actors.

The article explores the main forms and sources of pressure on Ukrainian media. Based on the analysis of reports from monitoring organizations (IMI, Detector Media, RSF, CPJ, Freedom House), as well as a qualitative analysis of high-profile cases of pressure on the editorial teams of Bihus.Info and "Ukrainska Pravda," the threats have been researched and systematized. It has been determined that external pressure from the Russian Federation is characterized by high aggression and includes massive cyberattacks, physical crimes against journalists, and the destruction of media infrastructure. Concurrently, the manifestations of internal pressure are examined, which has intensified and includes: political and administrative interference (attempts to influence editorial policy, use of mobilization as a tool of pressure), illegal surveillance and wiretapping, economic harassment (pressure on advertisers), and legal persecution.

In response to these challenges, the fundamental transformation of editorial crisis communication algorithms has been studied. The introduction of the concept of the "proactive crisis resistance model" is substantiated – an innovative strategy that goes beyond classical theories (SCCT, IRT), which have proven to be limited in the context of hybrid warfare.

It has been ascertained that the application of this model transforms crisis communication from a reputation management tool into a form of active resistance and a mechanism for ensuring institutional sustainability and protecting freedom of speech. The effectiveness of these strategies has been proven in mobilizing public support and in their ability to influence the authorities' reaction in specific high-profile cases, leading to the initiation of criminal proceedings and personnel decisions. At the same time, it is concluded that these strategies do not solve systemic problems, particularly the critical dependence on external funding and the general financial instability of editorial offices, which remains a key threat to their operational sustainability.

Key words: *crisis communication, online media, hybrid war, disinformation, pressure on journalists, freedom of speech, dual crisis, communication-resistance, proactive resistance model, media resilience.*

Дата надходження статті: 11.10.2025
Дата прийняття статті: 10.11.2025
Опубліковано: 29.12.2025