INFORMATION DIMENSIONS OF SOCIAL AND POLITICAL DISCOURSE

DOI: 10.46340/eppd.2021.8.1.21

Alina Datsenko
ORCID ID: https://orcid.org/0000-0002-5434-1471
National Institute for Strategic Studies, Kyiv, Ukraine

IMPLEMENTATION OF PRACTICAL MEASURES FOR EFFECTIVE PROTECTION OF THE INFORMATION SPACE OF UKRAINE IN CONDITIONS OF HYBRID WAR

Аліна Даценко
Національний інститут стратегічних досліджень, Київ, Україна

ВПРОВАДЖЕННЯ ПРАКТИЧНИХ ЗАХОДІВ ЕФЕКТИВНОГО ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

The article is devoted to the issues of countering Russian information aggression, aimed at destabilizing the internal political situation, reducing the ability of Ukraine and its people to resist the aggressor country.

The article proposes implementation of practical measures to protect the information space of Ukraine, related to the monitoring and analysis of information flows to detect and identify disinformation, propaganda, manipulations, etc.; the assessment of possible damage that may be caused by the implemented destructive information impact; elaboration and realization of coordinated and joint responses of public authorities, mass media and public organizations to the detected destructive information impact.

Systematic monitoring of data provides an opportunity to prevent and/or significantly reduce the destructive effects of disinformation materials. Qualitative detailed monitoring helps to determine the direction of the disinformation and propaganda campaign, its quantitative coverage and target audience. Having such insights, several scenarios of behavior (answers) can be developed in advance.

Responding to the dissemination of false (fake), inaccurate, distorted (manipulative) information (revealed by monitoring the information space) is possible only after verification and validation of such information (fact-checking) involving independent (non-profit) organizations that attract leading world authoritative experts and alternative means financing.

Assessing the degree of danger of destructive information impacts on the person, society, and state is necessary to further justification and implementation of measures to minimize their destructive impact, taking into account the economic and social capabilities of the country.

The comprehensive implementation of all measures of organizational, scientific and methodological, material and financial nature will increase the level of information security of the state in the conditions of information war.

Keywords: information war, information aggression, propaganda, disinformation, state policy in the field of information security, protection of information space, countering information aggression.

Постановка проблеми. Захист національного інформаційного простору неможливий без науково обґрунтованої стратегії та ефективної державної політики в інформаційній сфері, яка, у свою чергу, неможлива без визначеної системи національних цінностей, життєво важливих інтересів

в інформаційній сфері особистості, суспільства та держави, виявлення та постійного моніторингу актуальних загроз інформаційній безпеці держави, пошуку ефективних заходів для забезпечення інформаційної безпеки, захисту від інформаційних впливів та загроз і реалізації права на отримання достовірної інформації. При цьому захист інформаційного простору України наразі розглядається як один із основних напрямів державної інформаційної політики, від якого залежить існування суверенної України, її національна безпека, демократичний розвиток та відповідне місце у світовому співтоваристві.

Адже для нинішньої України реальним є гібридне протистояння з країною-агресором, яке дедалі більше впливає на усі сфери життєдіяльності українського суспільства включно з інформаційною політикою держави. Відповідно, на порядку денному є корегування або зміна пріоритетних напрямів реалізації державної інформаційної політики на більш практичні, які обумовлять якісні зміни в інформаційному просторі України. Звідси **завданням роботи** є розробка та впровадження заходів ефективного захисту інформаційному простору України в умовах гібридної війни.

Аналіз останніх досліджень і публікацій. Вітчизняними науковцями за час російської агресії проведено цілу низку досліджень, спрямованих на вдосконалення державної політики в сфері захисту інформаційного простору. Зокрема, А. Благодарний, О. Штельмах, Ф. Брецко в контексті стратегії гібридної війни та ознак і методів інформаційної агресії як її складової, виділяють такі аспекти протидії: постійний контроль інформаційного простору (преса, телебачення, радіо, Інтернет); обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією; посилення авторитету своєї влади, уряду, армії серед населення країни, аби перешкодити переходу на бік ворога та підтримці дій, які він нав'язує[1,2].

На думку В. Ліпкана «державна політика національної безпеки в інформаційній сфері має створювати умови для реалізації конституційного права громадян своєї держави вільно отримувати і використовувати інформацію для вирішення таких важливих завдань, як формування національного інформаційного простору, включення його до світового інформаційного простору на засадах забезпечення інформаційного суверенітету та інформаційної безпеки і формування демократично орієнтованої свідомості»[3].

У свою чергу, Д. Дубов у роботі «Державна інформаційна політика України в умовах гібридного миру та війни» пропонує такі пріоритети/цілі довгострокового характеру:

1) адаптація законодавства, що регулює інформаційну сферу та інформаційні відносини до реалій гібридного протистояння;

2) вироблення нової моделі функціонування медіа-середовища, яке б відповідало чинному етапу розвитку українського суспільства;

3) створення дієвої спеціальної державної інформаційної політики щодо окупованих територій та лінії розмежування;

4) розвиток медіа- та цифрової освіти на всіх рівнях;

5) реформування системи інформаційного позиціонування України на міжнародній арені в напрямі її більшої гнучкості та ефективності;

6) проведення реформи внутрішньої комунікативної діяльності держави та реформи урядових комунікацій;

7) розвиток потенціалу стратегічних комунікацій як механізму протидії деструктивній інформаційній діяльності щодо України[4].

Причому, автор зазначеної розробки зазначає, що вище наведений перелік не є вичерпним, оскільки не включає позитивістського порядку денного для державної інформаційної політики, пов'язаного із розвитком бібліотечної та архівної справи, підтримкою медіавиробництва та багатьма

[1] Благодарний, А. М., Штельмах, О. В. (2015). Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. *Інформаційна безпека людини, суспільства, держави*, *3*, 48-54.

[2] Брецко, Ф. (2015). Метою цієї війни є повне підпорядкування України експансіоністським неоімперським планам Кремля. *Prozak* <http://prozak.info/Suspil-stvo/Brecko-pro-gibridnu-vijnu-Rosiyi-proti-Ukrayini> (2020, червень, 14).

[3] Ліпкан, В. А. (2009). *Національна безпека України*. Київ: КНТ. *Бібліотека: політологія* <http://politics.ellib.org.ua/pages-8290.html> (2020, червень, 14).

[4] Дубов, Д. В. (2016). Державна інформаційна політика України в умовах гібридного миру та війни. *Стратегічні пріоритети*, *3,* 86-93.

іншими аспектами, оскільки тісно прив'язаний як до реальних викликів, що постали наразі перед Україною, так і до практичних можливостей країни.

Виклад основного матеріалу. Одною з основних складових російської гібридної війни є війна інформаційна, яка ведеться шляхом організації та практичної реалізації дезінформаційно-пропагандистських кампаній, деструктивних інформаційних вкидів, а також новинного маніпулятивного потоку задля перекручувань реальних подій у вигідному для країни-агресора контексті.

Розробка та впровадження заходів із протидії цим засобам інформаційної агресії має відбуватись з урахуванням європейського досвіду реалізації заходів протидії фейкам за допомогою системи RAS (Rapid Alert System) та на основі застосування якісного і кількісного попередньо обґрунтованих показників ефективності Системи швидкої протидії деструктивним інформаційним впливам, яка передбачає:

1) моніторинг та аналіз інформаційних потоків з метою виявлення та ідентифікації деструктивних інформаційних впливів (дезінформації, пропаганди, маніпуляцій, тощо);

2) оцінювання можливої шкоди (ризиків), якої може завдати впроваджений деструктивний інформаційний вплив, тобто комплексна оцінка пов'язаних з цим впливом небезпек для людини, суспільства, держави;

3) вироблення та реалізація скоординованих і спільно погоджених відповідей органів державної влади, ЗМІ та громадських організацій на виявлений деструктивний інформаційний вплив.

Як вважають експерти-аналітики, «моніторинг є одним з найпотужніших інструментів в боротьбі проти дезінформації та пропаганди. Тільки систематична робота з даними дасть можливість попередити інформаційні катастрофи та суттєво знизити їх руйнівний вплив. Деталізований моніторинг дозволить чесно поглянути на власні недоліки, працювати з ними та поступово їх усувати»[1].

На жаль, практично відсутні фундаментальні розробки прикладного характеру для спеціальної системи моніторингу інформаційного простору (ІП) (інтелектуального/технологічного комплексу) з метою вироблення сценаріїв різнорівневого управлінського застосування або використання існуючих пошукових систем саме для цієї мети. Водночас, окремі пошуковики спеціального спрямування стосуються лише деяких специфічних напрямів інформаційного впливу.

Тому ситуація із моніторингом ІП в органах державної влади залишається без зрушень, а сам моніторинг здійснюється на застарілій законодавчій базі та процедурно-регламентних рішеннях без ініціативних технологічних проривів. Незважаючи на кардинальні зміни, що відбулись за останні 6 років, усе відбувається в традиціях мирного часу та відповідно до застарілого законодавства[2].

У переважній більшості міністерств та відомств моніторинг інформаційного простору здійснюють або на первинному рівні (за тегами визначеної діяльності), або прес-служба простежує резонансні публікації, що стосуються відомства. Тобто, з точки зору системної роботи та випереджального аналітико-креативного сценарного реагування, такої діяльності немає[3].

Це пояснюється кількома чинниками:

– нерозумінням важливості формування відповідної стратегії комунікативно-контентного супроводу розвитку напряму діяльності на основі комплексного аналізу інформаційних потоків, що, у свою чергу, потребує оперативного осмислення подій, які висвітлюються в інформаційному просторі, та прийняття своєчасних, а за умов побудови інтелектуальних комплексів контекстового аналізу – випереджальних сценарних рішень;

– організаційно-штатні структури інформаційних підрозділів органів державної влади зазвичай є досить нечисленними та, відповідно, неспроможними виконувати серйозні аналітично-сценарні завдання;

– в органах державної влади бракує достатньої кількості високопрофесійних фахівців з питань моніторингу інформаційного простору та комунікативно-контентного забезпечення.

---

[1] Шара, А. (2019). Моніторинг проти пропаганди. *Блоги Liga.Net* <https://blog.liga.net/user/ashara/article/33167> (2020, червень, 17).

[2] *Закон України про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації, 1997* (Верховна Рада України). *Офіційний сайт Верховної Ради України*. <https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80#Text> (2020, червень, 16).

[3] Король, В. Г. (2015). Моніторинг заданої тематики інформаційного простору в центральних органах виконавчої влади: загальна характеристика особистості. *Інформаційне суспільство*, *22*, 56-61.

Таким чином, постає нагальна проблема зміни ставлення до моніторингу із заданої тематики інформаційного простору (як інноваційної технології) та переформатування (перенаціленння) структурних підрозділів, які виконують інформаційно-аналітичну роботу, на проведення якісного моніторингу ІП для виявлення та аналізу деструктивних інформаційних впливів.

Для реалізації зазначеного алгоритм дій у рамках загальної методології проведення комплексного моніторингу ІП[1] передбачає наступні кроки:

1. *Створення (виокремлення) моніторингової групи у складі інформаційно-аналітичного підрозділу*. У такій моніторинговій групі мають працювати фахівці з різноманітним досвідом та освітою. Лише у такому випадку можна забезпечити комплексну оцінку новин на етапі визначення змістовності чи кодування тем, що є необхідною й достатньою передумовою дотримання балансу різних упереджень, що зумовить більш об'єктивний погляд на контент ЗМІ.

2. *Розрахунок витрат (матеріальних, фінансових) на забезпечення роботи моніторингової групи*:

– гідна зарплата високопрофесійних фахівців групи;

– закупівля інформаційних матеріалів у компаній, що займаються медіааналітикою – записи ТБ- і радіо-програм, їх розшифровки, матеріали друкованих ЗМІ;

– програмне забезпечення для зберігання інформації (сервери, місце на хмарних сервісах, наприклад, Google Drive);

– витрати на публікацію результатів (у разі потреби).

3. *Формування вибірки джерел для моніторингу.* Через обмеження фінансових ресурсів невідворотним є формування вибірки найбільш релевантних ЗМІ. Утім, у більшості випадків аналіз усіх існуючих ЗМІ і не потрібен, адже репрезентативну картину медіаполя може дати вибірка джерел з найбільшим охопленням користувачів (найбільш рейтингові).

У вибірку ЗМІ у більшості випадків повинні потрапляти усі загальнонаціональні ЗМІ, що мають найбільше охоплення аудиторії. Для інтернет-ЗМІ можна скористатися відкритими рейтингами, що їх публікує на своєму сайті Інститут масової інформації: для телебачення – на сайті http://tampanel.com.ua/uk/contacts/ та для радіо – на сайті http://umediagroup.com.ua/analitics/show/1.

До вибірки також повинні потрапити ЗМІ з різними ідеологічними позиціями та ставленнями до діючої влади – як опозиційні, так і провладні.

У випадку тематичного моніторингу до вибірки необхідно додавати профільні видання, які спеціалізуються на даній тематиці або загалом сконцентровані на висвітленні суспільно-політичних, соціально-економічних та інших питань, які зачіпають інтереси широких верств населення.

Щойно вибірку джерел сформовано, можна обирати матеріали в них на наступній основі:

– інтернет та друковані ЗМІ: всі інформаційні секції та авторські колонки/блоги;

– телебачення та радіо: основні випуски новин; якщо в 24-годинному циклі є кілька випусків новинних програм, то слід вибрати ті, які мають найбільшу аудиторію. У першу чергу – випуски в прайм-тайм: для телебачення це 18:00-22:00, для радіо – 6:00-12:00.

Є певна можливість автоматизації частини процесу моніторингу, в першу чергу відбору публікацій, за допомогою RSS-агрегаторів (клієнтські програми, сервіси або веб-додатки для автоматичного збору повідомлень із джерел, які містять файли у форматі RSS або Atom, що відповідають за стрічки оновлень або новин на сайтах).

4. *Проведення класифікації джерел.* Після сформованої вибірки в залежності від завдань моніторингу необхідно класифікувати джерела за такими параметрами:

– географія: приналежність джерел до певного регіону/країни;

– власники медіа: приватні і державні/суспільні;

– за групами впливу.

5. *Обробка та аналіз текстових даних.* Після формування масиву матеріалів наступає етап безпосереднього кодування наявних публікацій. І якщо для класифікації джерел за територіальною приналежністю чи власником можна використати одноразово задані параметри (найбільш зручний спосіб для цього – відповідні формули в Microsoft Excel), то з визначенням змістовності все складніше. Щодо цього параметру потрібно оцінювати кожну окрему публікацію експертним шляхом.

[1] Кужель, Р. (2002). Методологія проведення моніторингу ЗМІ. *Council of Europe* <https://rm.coe.int/168047688d> (2020, червень, 18).

6. *Аналіз і обробка ТБ і радіо.* Принцип визначення змістовності повідомлень на ТБ і радіо досить подібний до того, що використовується при аналізі інтернет-ЗМІ. Якщо проводиться аналіз ТБ і радіо в простому текстовому форматі, то для зручності можна розбивати сюжети телеканалів на смислові блоки, виділяючи тематики кожного з них. У подальшому при написанні аналітичного матеріалу на основі моніторингу сюжети групуються за наявністю цих блоків і таким чином порівнюються події чи меседжі найбільше привернули увагу користувачів інформації.

Для впровадження заходів щодо оцінювання ризиків деструктивних інформаційних впливів, тобто ступеня їх небезпеки для людини, суспільства, держави, необхідно провести їхню формалізацію та подальше застосування методу експертних оцінок. Основою методу є ідея про те, що якщо певним чином зробити узагальнення та обробку індивідуальних оцінок експертів з приводу конкретної ситуації, то можна отримати загальну думку, в якій буде максимальна ступінь надійності та достовірності [1].

Головну складність при оцінюванні ризиків становить невизначеність просторово-часових характеристик процесів зародження і прояву джерел поділ деструктивних інформаційних впливів.

У теорії прийняття рішень розрізняються два типи невизначеності: статистичний і нестатистичний. До першого типу відносяться процеси, що можуть спостерігатися достатню кількість разів, зокрема, за допомогою натурних або модельних експериментів. Частота виникнення подій (інформаційних впливів), що характеризують ці процеси, трактується як статистична ймовірність. Якщо досліджувані процеси проявляються недостатню кількість разів, або взагалі припускають реалізацію лише в майбутньому, то їх слід віднести до нестатистичного типу невизначеності. У цьому випадку ймовірність трактується не як частота виникнення події, а як ступінь впевненості (міра можливості), що ця подія відбудеться. Нестатистична інтерпретація невизначеності оперує поняттям суб'єктивної ймовірності. Оцінювання суб'єктивних ймовірностей здійснюється за допомогою спеціально організованих експертних процедур на основі декомпозиції складної події на більш прості[2].

Узагальнена експертна процедура оцінювання ризиків інформаційних впливів докладно описана у роботі включає п'ять основних етапів:

1) ідентифікація джерел деструктивних інформаційних впливів. На цьому етапі виконуються такі заходи: збір та аналіз усіх доступних відомостей про випадки прояву і негативні наслідки інформаційних впливів з таких питань: (а) які за ґенезою є джерела деструктивних інформаційних впливів; (б) де, коли і за яких умов вони проявлялися чи можуть проявитися;

2) визначення стану джерел деструктивних інформаційних впливів, що передбачає проведення аналізу просторово-часових характеристик виявлених джерел з метою з'ясування: (а) яка була у минулому чи очікується частота виникнення і тривалість деструктивних інформаційних впливів від цих джерел на даній території при відсутності запобіжних заходів; (б) якими будуть зазначені характеристики при різних варіантах запобіжних заходів;

3) оцінка уразливості об'єктів впливу. На цьому етапі за результатами аналізу станів джерел деструктивних інформаційних впливів визначаються: (а) чисельність, склад і уразливість об'єктів впливу у межах даної території від можливих інформаційних загроз певного типу; (б) чисельність, склад і уразливість об'єктів впливу у межах даної території від можливих інформаційних загроз усіх типів;

4) визначення ризиків інформаційній безпеці. На основі проведеного аналізу стану джерел інформаційних загроз і потенційних об'єктів їх впливу формуються можливі сценарії зміни стану різних джерел і відповідні негативні наслідки їх прояву; прогнозуються – (а) якою може бути уразливість об'єктів впливу від усіх і від окремих типів інформаційних загроз; (б) якими будуть відповідні частоти прояву різних джерел інформаційних загроз;

5) обґрунтування заходів щодо мінімізації ризиків деструктивних інформаційних впливів. На заключному етапі з урахуванням економічних і соціальних вимог та можливостей розробляються питання: (а) який припустимий ризик, тобто припустима частота прояву різних джерел; (б) якими стануть сценарії зміни стану джерел інформаційних загроз і відповідні негативні наслідки їх прояву

[1] Куртов, А. І., Полікашин, О. В., Потіхенський, А. І. та інші (2017). Експертні оцінки. Метод "Делфі" як технологія прийняття управлінських рішень. *Збірник наукових праць Харківського університету Повітряних Сил*, *1,* 118-122.

[2] Бурячок, В. Л., Толюпа, С. В., Аносов, А. О та інші (2015). *Системний аналіз та прийняття рішень в інформаційній безпеці*. Київ: ДУТ.

після здійснення варіантів запобіжних заходів; (в) який варіант цих заходів забезпечує досягнення припустимого ризику при мінімальних витратах на їхню реалізацію[1].

Для формалізованого представлення ризику інформаційного впливу (R_{iv}) авторами розробки використовується модель, що пов'язує між собою ймовірність виникнення певних подій (прояву інформаційних джерел) (P) і відповідних їм наслідків (W):

$R_{iv} = P \cdot W$.

Враховуючи, що $0 \le P \le 1$ та нормовані втрати $0 \le W \le 1$, ці показники можна використовувати для кількісного оцінювання ризику інформаційного впливу в характерних ситуаціях:

1) $P = 1$, $W = 0$ – частота прояву інформаційної загрози велика, а величина втрат незначна: $R_{iv} = 0$;

2) $P = 0$, $W = 1$ – прояв інформаційної загрози відбувається вкрай рідко, а величина втрат велика: $R_{iv} = 0$;

3) $P = 0$, $W = 0$ – незначна частота прояву інформаційної загрози і її наслідків: $R_{iv} = 0$;

4) $P \neq 0$, $W \neq 0$ – відбуваються різні частоти прояву інформаційних загроз і різні наслідки: $R_{iv} \neq 0$.

Остання ситуація може оцінюватися як небезпечна і характеризуватися значною величиною ризику інформаційного впливу.

Для обчислення ймовірностей і, відповідно, оцінювання ризиків існують три основні методологічні підходи[2]:

– статистичний – за результатами багаторазових спостережень відповідно до закону великих чисел розраховують частоту прояву різних джерел негативних інформаційних впливів;

– соціологічний – визначається сприйняття населенням і його окремими групами тих чи інших інформаційних впливів. Проводяться соціологічні опитування, під час яких визначаються оцінки інформаційних ризиків, пов'язаних з прийняттям тих чи інших рішень щодо запобіжних заходів;

– експертний – у тих випадках, коли недостатньо статистичних даних щодо прояву різних джерел деструктивних інформаційних впливів; експерти дають суб'єктивні оцінки ймовірності прояву того чи іншого джерела.

Робота з деталізованими моніторингами ІП та експертними оцінками ризиків небезпеки інформаційних впливів допомагає визначити напрямок дезінформаційно-пропагандистської кампанії, її кількісне охоплення та цільову аудиторію. Володіючи такими інсайтами можна наперед розробити декілька сценаріїв поведінки (відповідей) органів державної влади, ЗМІ та громадських організацій:

1. *Негайна реакція*. Дезінформація вимагає швидкої відповіді. Заздалегідь визначаються канали передачі потрібних повідомлень. Це можуть бути списки медіа, журналістів (до яких є довіра), акаунти у соціальних мережах, підготовлені зразки заяв, брифінги для журналістів, документи, в яких спрогнозовані питання та відповіді на них. Всі ці кроки та інструменти повинні бути заготовленими і відтренованими до автоматизму.

2. *Зважена реакція*. Нерідко бувають ситуація, коли на дезінформаційно-пропагандистські кампанії не треба реагувати відразу. Адже в такі моменти можна потрапити в інформаційну пастку. В такому випадку доречно комбінувати інструменти негайної відповіді з повсякденною роботою в цьому напряму. Якщо в першому випадку доводиться працювати, в основному, вже з результатами кампанії, спрямованої проти нас, то у даному випадку, ми передбачивши основні напрямки ударів, працюємо на випередження. Тобто готуємо аудиторію до певних негативних меседжів, але ретельно їх дозуємо.

3. *Довгострокова стратегічна робота*. Розпланована покрокова стратегія дій на основі вивчених наслідків попередніх дезінформаційно-пропагандистських кампаній, встановлених алгоритмів їх проведення. Найбільш цінним тут є можливість прогнозування, а значить і попередження чи ефективної протидії поширенню дезінформації. Застосування сучасних технологій обробки мегаданих, отриманих за результатами якісного моніторингу, який може дати необхідні інструменти для формування як простих, так і складних інформаційних кампаній реагування[3].

Вітчизняні правознавці наголошують на проблемі, пов'язаній з тим, що часто уповноважені державою посадові особи не використовують передбачені законом правові механізми реагування

[1] Биченок, М. М., Войтко, О. В., Чернега, В. М. та інші (2017). Експертна процедура оцінювання ризиків негативних інформаційних впливів. *Сучасні інформаційні технології у сфері безпеки та оборони, 1*, 19-22.
[2] Саєнко, Ю. І. (2004). *Соціальні ризики та шанси. Соціальні ризики*. Київ: Фоліант, *2*.
[3] Шара, А. (2019). Моніторинг проти пропаганди. *Блоги Liga.Net* <https://blog.liga.net/user/ashara/article/33167> (2020, червень, 17).

на поширення дезінформації та пропаганди в українському інформаційному просторі. Зокрема, чинне законодавство України передбачає реагування на поширення неправдивої і недостовірної інформації (тобто дезінформації), причому реагування розділено на три рівні (цивільно-правова, адміністративна, кримінальна відповідальність), залежно від ступеня суспільної небезпеки поширення такої шкідливої інформації[1].

На думку науковців, ця проблема може бути вирішена лише через навчання відповідних посадовців і притягнення їх до відповідальності за бездіяльність у випадках, коли вони були зобов'язані вжити певних заходів.

Проте, реагування на поширення неправдивої (фейкової), недостовірної, перекрученої (маніпулятивної) інформації можливе лише після верифікації та перевірки такої інформації (фактчекінгу) із задіянням незалежних (некомерційних) організацій, які залучають провідних світових авторитетних експертів та альтернативні засоби фінансування.

Аналіз останніх досліджень свідчить про підвищений інтерес науковців і дослідників, а також журналістів-практиків до способів викриття неправдивого контенту в інформаційному просторі[2]. Українські медійники, спираючись на систему та алгоритми верифікації та фактчекінгу західних мас-медіа, пропонують власні стратегії виявлення брехні та перевірки фактів. На цій ниві активну роботу ведуть журналісти фактчекінгових проектів в Україні, що викривають фейки та маніпуляції Зокрема, «Слово і діло»[3] з 2008 р. перевіряє перевиборчі обіцянки політиків, у 2014 р. з'явилось дві платформи: StopFake.org для боротьби з фейками російської пропаганди та VoxUkraine, який аналізує економічні статті щодо залучення експертів, а з 2016 року діє аналог відомого американського порталу, який перевіряє на достовірінсть висловлювання українських політиків: «FactCheck-Ukraine»[4].

Фактчекери зазначають, що алгоритм викриття неправдивої інформації у різних організаціях хоча і має відмінності, проте концептуально базується на ключових моментах, що відрізняє фактчекінг від класичної схеми журналістського розслідування. Передусім це – повна відмова від використання в доказовій базі інсайдерської та неофіційної інформації. Для побудови дослідження фактчекінг користується тільки офіційними джерелами інформації, як українськими, так і зарубіжними, відповідями на запити в держоргани та зарубіжні інституції. Коментарі та експертні висновки використовуються в доказовій базі тільки в тому випадку, якщо вони спираються на документальні свідчення та дані з відкритих джерел[5].

Експерт фактчекінгового ресурсу StopFake.org О. Набожняк, розповідаючи про інструменти фактчекінгу, пропонує наступний алгоритм, що допомагає швидко і ефективно викривати брехню та спростовувати фейкові новини:

1. Обрати матеріал і виділити з нього твердження, що потребують перевірки, обрати якомога оперативніший та якісніший спосіб перевіряння.

2. Пошукати в авторитетних джерелах інформації підтвердження, що допоможуть класифікувати повідомлення як правдиве, неправдиве, оманливе або таке, що не можна перевірити.

3. Відібраний і проаналізований факт супроводжується коментарем, у якому аргументується вибір перевірки саме цього факту та її результат.

4. Експерт перевіряє коментар – якість і надійність джерела, відповідність класифікації.

5. Якщо коментар проходить перевірку, здійснюється перехресний фактчекінг (фінальна перевірка на внутрішню логіку); якщо ні – дослідник виправляє коментар, враховуючи зауваження експерта.

6. Залучення зовнішнього експерта, який, якщо це потрібно, оцінює текст.

7. Публікація перевірених даних. Публікуючи їх, слід посилатись на джерела перевірки та експертів[6].

---

[1] Сафаров, А. (2020). В Україні вже є законодавство і механізми щодо протидії дезінформації: заради чого колотнеча? *Інститут масової інформації.* <https://imi.org.ua/monitorings/v-ukrayini-uzhe-ye-zakonodavstvo-i-mehanizmy-shhodo-protydiyi-dezinformatsiyi-zarady-chogo-i31602> (2020, червень, 18).

[2] Кияшко, Ю. (2019). Фактчекінг як інструмент протидії маніпулятивному впливу електронних ЗМІ. *Вісник Львівського університету. Серія Журналістика, 45,* 28-35.

[3] Слово і діло (2020). *Головна сторінка* <www.slovoidilo.ua> (2020, червень, 17).

[4] Шевченко, В. (2018). Фактчекінг і верифікація у журналістській роботі. *Образ, 1 (27)*, 140-153.

[5] Гороховський, О. (2017). *Фактчек як тренд розслідувань: можливості та перспективи.* Дніпро: ЛІРА.

[6] Ейсмунт, В. (2016). Інструменти фактчекінгу: як професійно відрізняти брехню від правди. *Інститут масової*

Наукова співробітниця Центру Тоу Колумбійського Університету К. Вардл, досліджуючи соціальні медіа інформаційного простору, небезпечні своєю доступністю для широких мас, де автором може стати будь-хто і вдатися до маніпулятивних дій з інформацією, радить дотримуватись рекомендацій щодо перевірки контенту у соціальних медіа, зокрема, перевіряти та підтверджувати чотири елементи. По-перше, варто визначити походження інформації – чи дійсно цей фрагмент контенту оригінальний. По-друге, варто вивчити джерело контенту – проаналізувати, хто його завантажив. По-третє, перевірити дату контенту. Можливо, це застаріла інформація. По-четверте, перевірити місце розташування, де було створено продукт[1].

Експерт Лондонського бюро розслідувальної журналістики К. Блек наводить такий власний перелік ознак (не)достовірної інформації:

- особистість автора, його попередні статті, взаємодія з фахівцями і медіа;
- відсутність цитат із Wikipedia;
- дані лише з офіційних відкритих ресурсів;
- перевірка фотографій на достовірність: дата, погода, пейзаж, люди, одяг, тіні;
- приналежність сайту до конкретних людей із їхніми політичними перевагами;
- цитати не можуть бути вирвані з контексту;
- розрізнення фактичної інформації і думки автора статті чи коментарів (інтерв'юерів);
- цитати використовувати для пошуку першоджерела;
- експертна оцінка;
- перевірка інформації в архівах;
- прискіпливе ставлення до кожної деталі[2].

Втім, варто зазначити, що ці рекомендації не є вичерпними. Часто без допомоги додаткових інструментів важко визначити правдивість, оригінальність контенту. Особливо це стосується глибинних фейків. Журналісти The Wall Street Journal С. Маршал та Дж. Сарджент, які розробили свій звід правил, наголошують – часто геолокація дає інформацію про те, де і коли контент був завантажений у мережу, а не про те, де і коли він зроблений[3]. Так, журналісти не завжди можуть використовувати геолокацію під час верифікації інформації з соцмереж.

Щодо нашої країни, то важливо збільшувати охоплення тем, за якими перевіряються факти й дані, суттєво розширювати коло об'єктів для перевірки, тобто аналізувати не лише цифри та вислови, але й телевізійні програми, відеосупровід, фотографії, вузькопрофільні вислови, наприклад, про здоров'я, енергетичні проблеми, науку. Поширення фактчекінгу на всі сфери суспільного життя посилює контроль за окремими людьми і ЗМІ, відповідальність за сказане та написане. Крім цього, створення архіву неправдивих та маніпулятивних цитат чи матеріалів з детальним аналізом демонструє динаміку процесу та викриває персони, яким не можна довіряти[4].

Підсумовуючи викладене, слід ще раз підкреслити: у рамках впровадження практичних способів захисту інформаційного простору від деструктивних інформаційних впливів необхідно комплексно реалізувати вище зазначені заходи організаційного, науково-методичного та матеріального й фінансового характеру.

References:

1. Blahodarnyi, A. M., Shtelmakh, O. V. (2015). Orhanizatsiini aspekty protydii informatsiinii ahresii yak skladovoi hibrydnoi viiny [Organizational aspects of countering information aggression as a component of hybrid war]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy* [Information Security of the Person, Society and State.], *3*, 48-54. [in Ukrainian].
2. Bretsko, F. (2015) Metoiu tsiiei viiny ye povne pidporiadkuvannia Ukrainy ekspansionistskym neoimperskym planam Kremlia [Fedir Bretsko: The aim of this war is the complete subordination of Ukraine to the expansionist

інформації. <https://imi.org.ua/articles/instrumenti-faktchekingu-yak-profesiyno-vidriznyati-brehnyu-vid-pravdi/> (2020, червень, 19).

[1] Вардл, К. (2014). Перевірка контенту, отриманого від читачів. *Verification Handbook* <https://verificationhandbook.com/book_ua/chapter3.php> (2020, червень, 19).

[2] Кутовенко, О. (2016). 16 правил журналістського розслідування від експерта Лондонського Бюро розслідувальної журналістики. *MediaSapiens*. <https://ms.detector.media/profstandarti/post/16435/2016-04-15-16-pravil-zhurnalistskogo-rozsliduvannya-vid-eksperta-londonskogo-byuro-rozsliduvalnoi-zhurnalistiki/> (2020, червень, 23).

[3] Сухачева, А. (2015). Как проверять контент из соцсетей. Советы от Wall Street Journal, BBC и Reuters. *NewReporter* <https://newreporter.org/2015/10/29/kak-proveryat-proveryat-kontent-iz-socsetej-sovety-ot-wall-street-journal-bbc-i-reuters/> (2020, червень, 22).

[4] Шевченко, В. (2018). Фактчекінг і верифікація у журналістській роботі. *Образ, 1 (27)*, 140-153.

neo-imperial plans of the Kremlin]. *Prozak* <http://prozak.info/Suspil-stvo/Brecko-pro-gibridnu-vijnu-Rosiyi-proti-Ukrayini> (2020, June, 14).[in Ukrainian].
3. Lipkan, V. A. (2009). Natsionalna bezpeka Ukrainy [National Security of Ukraine]. *Biblioteka: politolohiya* [Library: political science]. Kyiv: KNT <http://politics.ellib.org.ua/pages-8290.html> (2020, June, 14). [in Ukrainian].
4. Dubov, D. V. (2016). Derzhavna informatsiina polityka Ukrainy v umovakh hibrydnoho myru ta viiny [State information policy in Ukraine in terms hybrid peace and war]. *Stratehichni priorytety* [Strategic Priorities], *3*, 86-93. [in Ukrainian].
5. Shara, A. (2019). Monitorynh proty propahandy [Monitoring against propaganda]. *Blog.Liga.Net* <https://blog.liga.net/user/ashara/article/33167> (2020, June, 17). [in Ukrainian].
6. *Zakon Ukrainy pro poriadok vysvitlennia diialnosti orhaniv derzhavnoi vlady ta orhaniv mistsevoho samovriaduvannia v Ukraini zasobamy masovoi informatsii, 1997* [Law on the Procedure for Covering Activities of Bodies of State Power and Local Self-Government by Mass Media in Ukraine, 1997]. (Verkhovna Rada Ukrainy) [(Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official site of the Verkhovna Rada of Ukraine]. <https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80#Text> (2020, June, 16). [in Ukrainian].
7. Korol, V. H. (2015). Monitorynh zadanoi tematyky informatsiinoho prostoru v tsentralnykh orhanakh vykonavchoi vlady: zahalna kharakterystyka osobystosti [Monitoring of the required issues of information space in the central executive authorities: general overview and features]. *Informatsiine suspilstvo* [Information society], *22*, 56-61. [in Ukrainian].
8. Kuzhel, R. (2002). Metodolohiia provedennia monitorynhu ZMI [Media Monitoring Methodology]. *Council of Europe* <https://rm.coe.int/168047688d> (2020, June, 18). [in Ukrainian].
9. Kurtov, A. I., Polìkashin, O. V., Potìhenskij, A. I. and others (2017). Ekspertni otsinky. Metod "Delfi" yak tekhnolohiia pryiniattia upravlinskykh rishen [Expert estimations. The method of "Delphi" as the technology of managerial decision-making]. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl* [Scientific works of Kharkiv national air force university], *1*, 118-122. [in Ukrainian].
10. Buriachok, V. L., Toliupa, S. V., Anosov, A. O. and others (2015). *Systemnyi analiz ta pryiniattia rishen v informatsiinii bezpetsi* [System analysis and decision-making in information security]. Kyiv: DUT. [in Ukrainian].
11. Bychenok, M.M., Voytko, V.V., Cherneha, V.M. and others (2017). Ekspertna protsedura otsiniuvannia ryzykiv nehatyvnykh informatsiinykh vplyviv [Expert risk assessment procedure of negative information impacts]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony* [Modern Information Technologies in the Sphere of Security and Defence], *1*, 19-22. [in Ukrainian].
12. Saienko, Yu. I. (2004). Sotsialni ryzyky ta shansy [Social risks and chances]. *Sotsialni ryzyky* [Social risks]. *2*, Kyiv: Foliant. [in Ukrainian].
13. Safarov, A. (2020). V Ukraini vzhe ye zakonodavstvo i mekhanizmy shchodo protydii dezinformatsii: zarady choho kolotnecha? [Ukraine already has legislation and mechanisms to counter disinformation: what is the fight for?] *Instytut masovoi informatsii* [Institute of Mass Media]. <https://imi.org.ua/monitorings/v-ukrayini-uzhe-ye-zakonodavstvo-i-mehanizmy-shhodo-protydiyi-dezinformatsiyi-zarady-chogo-i31602> (2020, June, 18). [in Ukrainian].
14. Kyiashko, Y. (2019). Faktchekinh yak instrument protydii manipuliatyvnomu vplyvu elektronnykh ZMI. [Factchecking as an instrument which would counter the manupulative influence of electronic media]. *Visnyk Lvivskoho universytetu. Seriia Zhurnalistyka* [Visnyk of the Lviv University. Series Journalism], *45*, 28-35. [in Ukrainian].
15. Shevchenko, V. (2018). Faktchekinh i veryfikatsiia u zhurnalistskii roboti [Factcheking and verification in the journalism activity]. *Obraz*, *1 (27)*, 140-153. [in Ukrainian].
16. Horokhovskyi, O. (2017). *Faktchek yak trend rozsliduvan: mozhlyvosti ta perspektyvy* [Factcheck as an investigation trend: opportunities and prospects] . Dnipro: LIRA. [in Ukrainian].
17. Eismunt, V. (2016).Instrumenty faktchekinhu: yak profesiino vidrizniaty brekhniu vid pravdy [Factchecking tools: how to professionally distinguish false from truth]. *Instytut masovoi informatsii* [Institute of Mass Media]. <https://imi.org.ua/articles/instrumenti-faktchekingu-yak-profesiyno-vidriznyati-brehnyu-vid-pravdi/> (2020, June, 19). [in Ukrainian].
18. Vardl, K. (2014). Perevirka kontentu, otrymanoho vid chytachiv [Verifying User-Generated Content]. *Verificationhandbook* <https://verificationhandbook.com/book_ua/chapter3.php> (2020, June, 19). [in Ukrainian].
19. Kutovenko, O. (2016). 16 pravyl zhurnalistskoho rozsliduvannia vid eksperta Londonskoho Biuro rozsliduvalnoi zhurnalistyky [16 investigative journalism rules from the London Bureau of Investigative Journalism expert]. *MediaSapiens*. <https://ms.detector.media/profstandarti/post/16435/2016-04-15-16-pravil-zhurnalistskogo-rozsliduvannya-vid-eksperta-londonskogo-byuro-rozsliduvalnoi-zhurnalistiki/> (2020, June, 23). [in Ukrainian].
20. Sukhacheva, A. (2015). Kak proveriat kontent iz sotcsetei. Sovety ot Wall Street Journal, BBC i Reuters[How to check content from social networks. Tips for verifying eyewitness media from WSJ, BBC and Reuters]. *NewReporter*. <https://newreporter.org/2015/10/29/kak-proveryat-proveryat-kontent-iz-socsetej-sovety-ot-wall-street-journal-bbc-i-reuters/> (2020, June, 22). [in Russian].