Chapter 13

ДЕЗІНФОРМАЦІЯ У ЗМІ: ВИКЛИКИ ТА ТЕХНОЛОГІЇ ПРОТИДІЇ В УМОВАХ ВІЙНИ

Негребецький В. В.
DOI https://doi.org/10.30525/978-9934-26-554-9-13

ВСТУП

В умовах сучасної гібридної війни інформація стає не просто інструментом комунікації, а справжньою зброєю, здатною впливати на масову свідомість, дестабілізувати суспільство та підривати довіру до державних інституцій. Дезінформація як ключовий елемент цього інформаційного протистояння широко використовується ворожими силами для маніпуляції суспільною думкою, створення паніки і поширення фейків.

Особливо гостро ця проблема стоїть в Україні, де війна ведеться не лише на полі бою, а й у медіапросторі. Вороги держави активно використовують пропаганду, фальшиві новини та спотворену інформацію для послаблення морального духу громадян та міжнародної підтримки. У таких умовах пошук ефективних методів боротьби з дезінформацією стає стратегічно важливим завданням.

Метою дослідження є проаналізувати проблему дезінформації у сфері засобів масової інформації в умовах війни в Україні, виявити основні механізми її поширення та оцінити сучасні технології, що використовуються для протидії інформаційним атакам. В рамках дослідження також розглядаються державні ініціативи, міжнародний досвід та перспективні стратегії захисту інформаційного простору, спрямовані на мінімізацію впливу дезінформації та зміцнення медійної стійкості суспільства[1].

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Указом Президента України від 28 грудня 2021 року №685/2021 було затверджено Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про

[1] Примітка. Стаття написана у межах розробки фундаментальної теми «Пріоритезація та технологізація у кримінальному провадженні у воєнний та повоєнний час», яка досліджується фахівцями НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України.

Стратегію інформаційної безпеки України»[2]. Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Реалізація Стратегії розрахована на період до 2025 року.

Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина.

21 сторіччя характеризується стрімким розвитком інноваційних цифрових технологій, метою яких є підвищення ефективності діяльності людини, покращення комфорту і результатів праці. Розвиток інформаційного простору в умовах глобалізації та пандемія COVID-19 зумовили посилення ролі соціальних мереж у національному та світовому інформаційному просторі, їх вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини, зокрема щодо забезпечення принципів рівності прав користувачів соціальних мереж.

Принаймні право на приватність (захист конфіденційної інформації про особу, невтручання в особисте життя) є одним з основних прав людини, що закріплено в Загальній декларації прав людини, Конвенції про захист прав людини і основоположних свобод, інших міжнародних документах, а також конституціях більшості держав світу, цифрові трансформації змінюють і цю сферу. Збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність. Спроби врегулювати цю проблему тривають, формуються нові підходи у забезпеченні балансу права на приватність та інформаційної безпеки держави.

Значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди, популярності

[2] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.

конспірологічних теорій. Некритичне сприйняття інформації створює загрози політичній та економічній стабільності демократичних держав.

Питанням правового забезпечення безпеки в інформаційному просторі та протидії спеціальним інформаційним операціям у контексті діяльності сектору безпеки й оборони України були присвячені роботи багатьох вітчизняних фахівців з інформаційної безпеки, таких як О.О. Верголяс, Д.В. Вєдєнєєв, О.Г. Заруба, Ю.І. Когут, О.М. Лебедєв, О.В. Литвиненко, В.А. Ліпкан, Н. В. Нетеса, В.В. Мокляк, В.Я. Новицький, В.М. Панченко, О.П. Дзьобань, В.Г. Пилипчук, В.М. Фурашев, Д.В. Ланде та ін.[3].

За останні роки ставлення до інформаційної безпеки України зазнало значних змін. Насамперед трансформувалася сама природа цього явища, а разом із нею – і стратегічний вимір концепції забезпечення національної інформаційної безпеки. Сьогодні вона вже не сприймається як щось абстрактне чи винятково теоретичне. Навпаки, це реальна і вкрай гостра сфера протистояння, в якій розгортаються запеклі бої, а погрози мають цілком конкретні та відчутні наслідки.

В умовах масштабної інформаційної війни проти України, одним із ключових викликів стає правове забезпечення стратегічної концепції інформаційної безпеки. Довоєнні напрацювання у цій сфері стали важливою основою для подальшого розвитку та наукових досліджень. Однак сучасні реалії вимагають не просто переосмислення існуючих підходів до правового регулювання інформаційної сфери, а й усвідомлення того, що правова складова національної безпеки залежить від захищеності інформаційного простору. При цьому окремі аспекти правового забезпечення інформаційної безпеки в умовах воєнного стану залишаються недостатньо вивченими. Це потребує більш детального аналізу даної проблематики, що дозволить як поглибити наукове розуміння питання, а й виробити ефективні механізми протидії сучасним загрозам.

Слід відзначити, що в літературних джерелах та на наукових заходах в основному розглядались окремі аспекти використання сучасних інноваційних цифрових технологій в контексті забезпечення інформаційної безпеки[4]. Разом із тим, не всі існуючі на даний час технології були предметом дослідження, тому потребує подальшого

[3] Нетеса Н. В., Мокляк В. В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право.* 2023. № 3(46). С. 98–107. URL: http://il.ippi.org.ua/article/view/287168

[4] Інформаційна безпека: сучасний стан, проблеми та перспективи: збірник матеріалів Міжнародної науково-практичної конференції. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с. URL: https://politkaf.kpnu.edu.ua/wp-content/uploads/2023/04/zbirnyk-material-konfer.-inf_bezp_2023.pdf

дослідження питання використання інформаційних технологій, зокрема сучасні технології виявлення та протидії фейкам. Також актуальною залишається проблема використання цифрових доказів, оскільки на відміну від традиційних «не цифрових» доказів, всі ці документи утворюються цифровими засобами і зберігаються на цифрових платформах. У зв'язку з війною в Україні вкрай актуальним постає питання розробки і впровадження перспективної стратегії захисту інформаційного простору України. Це пояснюється тим, що війна проти України з самого початку мала «гібридний» характер, тобто одночасно використовувались інформаційні атаки та диверсії в комунікативних мережах, тому вельми актуальним є дослідження питання протидії спеціальним інформаційним операціям.

1. Дезінформація у ЗМІ як інструмент гібридної війни

Початок військової агресії проти України в 2022 році був тісно пов'язаний з сильним інформаційним впливом ворога на наше суспільство через технології гібридних війн. Це сталося можливим завдяки активному використанню інформаційних технологій, та впливу інноваційних інструментів обміну та передачі інформації в різноманітних інформаційних ресурсах.

Нажаль не всі технології інформаційного пошуку однаково рівноцінні, безпечні і стійки до незаконного інформаційного впливу. В 2023 році компанія Google впровадила технологію Search Generative Experience (SGE)[5]. Цей пошуковий сервіс ретельно розроблений та навчений виявляти й представляти користувачеві високоякісні результати, які відповідають інформації у видачі та підтримують її. Об'єднавши найсучасніші поєднання мовних моделей і цілеспрямовані методики навчання, компанія Google створила пошукову систему, яка надає надійну і підтверджену інформацію. Google прагне запобігати демонстрації шкідливого, образливого або відвертого контенту у своїх системах ранжування. Технологія Search Generative Experience (SGE), на які ґрунтуються пошук, створена саме для цього. Основна увага приділяється створенню інформативних відповідей, підтверджених надійними джерелами, щоб користувачі отримували правдиву і перевірену інформацію. У випадках, коли системи Google мають меншу довіру до джерела або стикаються з інформаційними прогалинами, мета полягає в тому, щоб уникнути надання знімків, згенерованих штучним інтелектом. Крім того, відверті або небезпечні теми навмисно уникаються, щоб підтримувати відповідальне та безпечне середовище пошуку.

[5] Новий алгоритм пошуку Google на основі AI: чого очікувати (29.10.2023). URL: https://livepage.ua/blog/the-new-ai-powered-google-search-what-to-expect.html.

Безумовно технології персоніфікованого підбору відомостей мають велике майбутнє, надають багато переваг особам, що навчаються або підвищують свій професійний рівень. Але нажаль будь-який інструмент в руках правопорушника може перетворитись на зло. І якщо йдеться про інформаційні технології, то сила цього лиха збільшується у багато разів. Так, месенжери, а також соціальні мережі, доступ до яких має майже кожний, надають найбільше можливостей для поширення практично будь-якої інформації. Є можливість не просто одноразово поширити новину, а запустити «ланцюжкову реакцію», коли новина багаторазово пересилається користувачами соц. мережі від однієї особи до цілою групи осіб, або навіть до інших соц. мереж.

Шкода, що не всі інформаційні ресурси здатні виявляти ненадійні джерела інформації. Новини та повідомлення можуть не відповідати дійсності[6]. Фейк у перекладі з англійської «fake» означає − «фальшивка», «підробка», «обман». Таким чином, фейк − це завідомо неправдива інформація. Дезінформація – відомості, що розраховані на введення особи в оману[7].

Визначають три види інформації, яка може охарактеризувати фейки:

− дезінформація (disinformation) – неправдива та свідомо створена для заподіяння шкоди людині, соціальній групі, організації чи країні інформація;

− неправдива інформація (misinformation) – помилкова, але створена без наміру завдати шкоди, інформація;

− спотворена інформація (malinformation) – інформація, що ґрунтується на реальних фактах, використовується для заподіяння шкоди особі, організації або країні[8].

Особливого значення набуває питання про відповідальність за поширення інформації, яка загрожує Національній безпеці України, а саме спрямованої на заподіяння шкоди суверенітетові, територіальній цілісності та недоторканості, обороноздатності, державній, економічній чи інформаційній безпеці держави. Таким чином, ворог намагається методично і послідовно підірвати авторитет держави і органів влади, і послабити обороноздатність країни. В пояснювальній записці до законопроекту №9223 від 19 квітня 2023 р. «Про внесення

[6] Аналітичний звіт «російський інформаційний вплив в Африці». URL: https://cpd.gov.ua/reports/analitychnyj-zvit-rosijskyj-informaczijnyj-vplyv-v-afryczi/.

[7] Велика українська юридична енциклопедія: У 20 т. Т.20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків: Право, 2018. 952 с.

[8] Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making (2nd edn, CoE 2008). URL: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України» повідомляється, що «російськими спецслужбами в інтересах країни-агресора нарощуються зусилля із використання такого інструменту інформаційної війни як створення на платформах соціальних мереж Facebook, Instagram і Twitter мереж облікових записів (акаунтів) (так званих бот-мереж), які містять недостовірні дані щодо користувачів, діяльність яких є координованою ззовні та об'єднана єдиною метою, зокрема такою як проведення акцій інформаційного впливу проти державних інтересів України. До таких дій вдаються і громадяни України. Так, Службою безпеки України виявлено та припинено функціонування за 2022 рік – 45 ботоферм, загальною потужністю понад 4 млн. ботів, діяльність яких поширювалась на багатомільйонні аудиторії користувачів соціальних мереж у різних регіонах України (і не лише). Разом з тим, вжитими заходами було викрито та заблоковано близько 11 тис. облікових записів, що використовувались на користь російських окупантів. Непоодинокими стали і випадки, коли користувачі облікових записів (акаунтів) видають себе за інших осіб, зокрема за представників влади, інших публічних осіб, до яких прикута особлива увага, і від імені цих осіб розміщують і поширюють в соцмережах та на інших інтернет-платформах різну неправдиву, маніпулятивну інформацію.

Окрім цього, зі зростанням впливу соціальних мереж загострилася проблема «інформаційних бульбашок», коли люди оточені лише інформацією, яка підтверджує їхні власні погляди та переконання. Це явище може створювати ілюзію однакового мислення в групі людей і призводити до ізольованості від інших поглядів, зменшення різноманітності думок та навіть загострення конфліктів. При цьому, люди схильні створювати навколо себе «інформаційні бульбашки»: блокують у соцмережах або не сприймають контент, який не відповідає їхнім уподобанням. Також вони активніше реагують і поширюють те, що відповідає їхнім інтересам і емоціям. Алгоритми соцмереж підлаштовуються під такі бажання користувачів і з часом взагалі перестають пропонувати в стрічці альтернативні погляди. Так, подивившись кілька разів певний контент, алгоритми соцмережі надалі активніше пропонуватимуть саме таку інформацію[9].

[9] Як не стати жертвою шахраїв та ворожої пропаганди: кіберполіція про фактчекінг (02 травня 2024 р.). URL: https://cyberpolice.gov.ua/article/yak-ne-staty-zhertvoyu-shaxrayiv-ta-vorozhoyi-propagandy-kiberpolicziya-pro-faktcheking-437/

На жаль, соціальні мережі не дуже реагують на повідомлення про фейкові профілі і сторінки, які причетні до інформаційних атак»[10]. Тому існує необхідність підвищити контроль з боку правоохоронців. Якщо інформація розміщена у вільному доступі, є можливість використовувати методику збирання й аналізу інформації з відкритих джерел (*Open source intelligence, OSINT*).

Протидія такій витонченій дезінформації вимагає не лише технологічних рішень, а й комплексного підходу. Підвищення медіаграмотності має вирішальне значення для того, щоб громадськість могла ідентифікувати і розуміти тактики, які використовуються в дезінформаційних кампаніях. Соціальні медіа-платформи також повинні взяти на себе відповідальність, вдосконалюючи виявлення та видалення фейкових акаунтів і співпрацюючи з фактчекерами для забезпечення прозорої модерації контенту. Крім того, регуляторне середовище має розвиватися, щоб покласти на соціальні медіаплатформи відповідальність за контент, який вони поширюють, і захистити дані користувачів від експлуатації. Урядам і міжнародним організаціям слід розглянути нормативно-правові акти, які вирішують ці проблеми, балансуючи між потребою у свободі вираження поглядів та імперативом збереження цілісності інформації[11].

Насамкінець, необхідно підкреслити важливість пильності, технологічної грамотності та дотримання етичних стандартів у складній взаємодії наративів та штучного інтелекту в соціальних мережах. Для журналістів, творців контенту і користувачів соціальних мереж розуміння цієї динаміки є ключем до ефективної протидії дезінформації та відстоювання правди в нашому все більш взаємопов'язаному світі.

Соціальні медіа-платформи, такі як Facebook та X (колишній Twitter), стали ключовими гравцями в ландшафті дезінформації, керованої штучним інтелектом. Поява генеративного ШІ значно посилила поширення і витонченість дезінформаційних кампаній. Ці кампанії все частіше використовують інструменти штучного інтелекту для створення та поширення оманливої інформації в безпрецедентних масштабах. Також ці медіа-платформи стикаються з проблемою модерації контенту, створеного штучним інтелектом.

---

[10] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України: Законопроект України від 19.04.2023 № 9223 / База даних «Законодавство України / ВР України. URL: itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk_RIKKEZHmqd699_G6ZH0h9ZmxhEwLZ_ZpXM61T0/.

[11] Посібник для творців контенту для виявлення та протидії російській пропаганді в нових технологіях. (За підтримці Уряду Великої Британії в рамках проекту «Розуміння штучного інтелекту). 2024. URL: https://ai.instingov.org/assets/guide/AI-Guide_uk.pdf

2. Сучасні технології виявлення та протидії дезінформації

У сучасному інформаційному просторі, де дезінформація становить серйозну загрозу демократичним процесам, роль фактчекінгу стає як ніколи важливою. Сьогодні спостерігається зростаючий інтерес до вивчення механізмів виявлення фальсифікацій в медіа як з боку академічної спільноти, так і серед практикуючих журналістів. Українські медіаексперти, спираючись на передовий міжнародний досвід у галузі фактчекінгу та верифікації інформації, активно адаптують та вдосконалюють власні методики розпізнавання неправдивих заяв.

Фактчекінг – це процес перевірки інформації на достовірність. Фактчекінг став невід'ємною частиною сучасної журналістики та повсякденного життя. В епоху, коли інформація поширюється зі швидкістю світла, важливість перевірки фактів неможливо переоцінити. Згідно з дослідженням американської організації «Duke Reporters' Lab», на сьогодні функціонує 446 фактчекінгова організація в різних країнах світу[12].

Фактчекер перевіряє інформацію виключно на основі відкритих і офіційних джерел. Ключова відмінність факторингу від журналістських розслідувань полягає в принциповій відмові від використання інсайдерської, анонімної або неофіційної інформації в якості доказової бази. У процесі перевірки фактчекери спираються на офіційні дані українських і зарубіжних державних органів, міжнародних організацій, наукових інститутів, а також на офіційні відповіді на запити, спрямовані до відповідних установ.

Для перевірки інформації фактчекери використовують дані з офіційних джерел, таких як:

Державна служба статистики України,
Міністерство фінансів України,
Державна казначейська служба України,
Верховна Рада України,
Кабінет Міністрів України,
Національний банк України,
Міжнародний валютний фонд,
Світовий банк та інші авторитетні організації.

Додаткові рекомендації щодо верифікації інформації представлені в «Посібнику з верифікації» (Verification Handbook), виданому Європейським центром журналістики[13]. У цьому посібнику визнані світовою спільнотою редактори і журналісти діляться методиками перевірки контенту на достовірність. Воно містить перелік онлайн-

[12] Fact-Checking. URL: https://reporterslab.org/fact-checking/

[13] Посібник з верифікації. Центр Європейської Журналістики; Асоціація Видавців (УАВПП). 2014. URL: https://verificationhandbook.com/book_ua

інструментів, що дозволяють верифікувати: текстові публікації, фото – та відеоматеріали, першоджерела інформації, особу розповсюджувачів інформації, акаунти в соціальних мережах.

Фактчекінг є однією з різновидів журналістського розслідування і включає в себе основні структурні елементи, аналогічні традиційному журналістському аналізу. До них відносяться:

1. Об'єкт дослідження – перевіряється твердження, факт або інформація.

2. Доказова база-офіційні дані, документи та підтверджені джерела.

3. Посилання на компетентні джерела-державні органи, наукові інститути, міжнародні організації та інші авторитетні ресурси.

4. Коментарі експертів-думки фахівців, що сприяють об'єктивній оцінці інформації.

5. Логічний висновок – підсумковий висновок про достовірність перевіряється факту[14].

Фактчекінг складається з декількох ключових смислових блоків:

1. Об'єкт перевірки – публічна заява (рідше – резонансний факт), що піддається дослідженню;

2. Суть питання – інформаційна преамбула, що містить роз'яснювальні матеріали, що передують доказовій базі;

3. Докази і аргументи – підтверджені факти, статистичні дані, документи і свідоцтва, отримані виключно з відкритих офіційних джерел, а також експертні думки, підкріплені посиланнями на авторитетні ресурси;

4. Вердикт – підсумковий висновок про достовірність інформації з коротким аргументованим поясненням.

Вердикт у фактчекінгу має чітку структуровану форму і заснований на об'єктивних критеріях, що дозволяє уникнути суб'єктивності та оціночних суджень. В українській практиці використовуються три типи вердиктів:

1. «Правда» – інформація відповідає фактам;

2. «Напівправда» – інформація містить як достовірні, так і спотворені або маніпулятивні елементи;.

3. «Неправда» – інформація повністю недостовірна.

Базовий протокол верифікації інформації для фактчекерів включає кілька послідовних етапів:

1. Визначення матеріалу – виявлення тверджень, що вимагають перевірки.

[14] Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи: Практичний посібник. Дніпро : ЛІРА, 2017. 133 с.

2. Вибір методу перевірки – визначення найбільш швидкого і ефективного способу верифікації.

3. Пошук інформації -– аналіз даних з визнаних авторитетних джерел для підтвердження або спростування факту, класифікації його як правдивого, помилкового, маніпулятивного або сумнівного.

4. Аналіз та обґрунтування – вивчення відібраного факту з аргументованим обґрунтуванням обраного методу перевірки та поданням результатів.

5. Експертна перевірка-оцінка надійності джерел і коректності їх класифікації.

6. Перехресний фактчекінг – фінальна перевірка логічної послідовності інформації. У разі невідповідностей матеріал коригують з урахуванням експертних зауважень.

7. Залучення зовнішніх експертів (за необхідності) для додаткової оцінки тексту.

8. Публікація перевіреної інформації – подання остаточних даних з обов'язковими посиланнями на джерела і з зазначенням вкладу експертів в процес верифікації[15].

Серед фактчекінгових платформ українських розробників необхідно відзначити платформу Mantis Analytics (2023)[16]. Остання за допомогою штучного інтелекту виявляє фейкову інформацію та дезінформацію в онлайн-медіа та соцмережах. Mantis у режимі реального часу обробляє тисячі повідомлень та гігабайти даних, а потім представляє дані на інтерактивній карті.

В 2022 році в месенджері Telegram було запущено фактчек-бот «Перевірка»[17]. Центр протидії дезінформації при РНБО України рекомендує цей бот-рятівник від фейкових новин, неперевіреної інформації[18]. Для перевірки інформації досить переслати новину боту. Команда фактчек-відділу Ґвара Медіа опрацьовує інформацію, яку надсилають користувачі бота «Перевірка» та факти, що є віральними або суспільно-небезпечними. Запитам, що надходять у бот «Перевірка» фактчекери можуть присвоїти 5 статусів, а також відправити його на більш глибинну перевірку. Можливі статуси: Правда; Фейк; Напівправда; Немає доказів; Відмова.

[15] Ейсмунт В. Інструменти фактчекінгу: як професійно відрізняти брехню від правди. Інститут масової інформації. URL: https://imi.org.ua/articles/instrumenti-faktchekingu-yak-profesiyno-vidriznyati-brehnyu-vid-pravdi-i407

[16] Mantis Analytics. URL: https://mantisanalytics.com/

[17] Фактчек-бот "Перевірка". URL: https://t.me/perevir_bot

[18] Центр протидії дезінформації при РНБО рекомендує новий фактчек-бот «Перевірка» (18.03.2022). URL: https://imi.org.ua/news/tsentr-protydiyi-dezinformatsiyi-pry-rnbo-rekomenduye-novyj-faktchek-bot-perevirka-i44450

Правда означає, що інформація відображає реальну ситуацію в житті, не спотворюючи жодного її аспекту. Правдива інформація – фактологічно достовірна, подана в правильному контексті.

Статус «Правда» передбачає, надійні джерела підтверджують інформацію. При цьому передбачається, що фактчекер обрав для підтвердження факту більше ніж одне джерело, окрім випадків коли джерело є єдиним, що висвітлює дану тему.

Фейк означає, що ця інформація повністю недостовірна, вигадана, оманлива – відповідних подій, ситуацій, явищ взагалі не було. Брехлива інформація є такою, чию фейковість можна довести.

Напівправда (Маніпуляція) – твердження, яке містить елементи правди та неправди в тих чи інших пропорціях. Напівправдива інформація вводить аудиторію в оману шляхом подачі інформації у спотвореному контексті. Запити, що здобувають статус «Напівправда», потребують коментаря – стислого аналізу основних колізій між правдивими та неправдивими даними.

Бракує доказів – інформація, яка не може бути жодним чином підтверджена доказами. У інформації з таких запитів немає надійного підтвердження у відкритому доступі.

Відмова це статус, який отримує запит, що неможливо перевірити через технічні чи інші причини. Так відмову варто залишати якщо:

1. Не містить проблемних фактів (у запиті – лише назва бренду, покликання на фотографію без супровідного тексту);
2. Недоступна (застаріле або заблоковане покликання);
3. Запит є неконструктивним (маячня, неетичність, розвага);
4. Інформацію неможливо перевірити в режимі реального часу (дані про взліт бомбардувальників, чи звуки вибухів в регіоні).

Додаткова функція – «Ескалація». *Ескалація* – це додаткова функція, що необхідна для того, щоб окреслити потребу у більш детальній перевірці даного запиту. При використанні даної функції користувач буде повідомлений про те, що його запит потребує більше часу для аналізу. Після обробки запиту йому варто присвоїти один з вищенаведених статусів: правда, фейк, напівправда чи бракує доказів.

Після присвоєння статусу фактчекер за потреби надає коментар. Коментар до відповіді – лаконічний текст, що обґрунтовує, роз'яснює присвоєний запиту статус. Надаючи коментар на запит, фактчекер формує його з дотриманням політики фактчекінгу, що наслідує фактчек-відділ Gwara Media. Коментар містить пояснення та покликання на джерела, на підставі яких зроблено висновки. Отриманий користувачем коментар дає змогу йому самостійно перевірити правильність наданої фаткчекером інформації через відтворення шляху пошуку цієї інформації.

Швидкість перевірки запитів відбувається згідно наступного розподілу:

«швидкі запити» – опрацьовуються не довше, ніж 24 год, оскільки відповідь на цей запит є загальнодоступною та не потребує детальної технічної перевірки;

«повільні запити» – визначаються присвоєнням статусу ескалації та опрацьовуються протягом 7 днів, оскільки є потреба у проведенні глибинного аналізу інформації.

Фактчекер може зв'язатися з користувачем для уточнення запиту**.** Для цього у боті існує функція «діалог з ініціатором». Вона ініціює повідомлення користувачу від імені фактчекера через бот. При цьому, варто зауважити, персоналія ініціатора не відстежується, оскільки комунікація відбувається саме через діалог у боті.

Згідно з політикою фактчекінгу на сайті фактчек-відділу спростування фейкових новин, що мають ознаки віральної чи небезпечної складової. Опублікований матеріал може мати статус «Фейк» чи «Напівправда» (маніпуляція). Перевірка відбувається аналогічно до методології перевірки запитів з бота[19].

3. Перспективи та стратегії інформаційного захисту в Україні

Нормативно-правове регулювання інформаційної безпеки, зокрема і в інформаційній мережі Інтернет здійснюється Конституцією України, законами України, указами Президента та постановами КМУ і ВРУ. Основу інформаційного законодавства складають, зокрема, Закони: «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», «Про Національну поліцію», «Про національну інфраструктуру геопросторових даних», «Про доступ до публічної інформації», «Про основні засади забезпечення кібербезпеки України».

Підзаконні нормативно-правові акти у сфері інформаційної безпеки відіграють ключову роль системі правового регулювання, забезпечуючи практичну реалізацію стратегічних рішень. Вони встановлюють конкретні правила, процедури та стандарти, які деталізують та доповнюють основні принципи, закладені у державних стратегіях та програмах. Завдяки цим актам діяльність державних органів, підприємств та інших суб'єктів стає більш системною та впорядкованою, що сприяє ефективному впровадженню політики інформаційної безпеки. Такий підхід дозволяє не тільки підвищити рівень захищеності інформаційних

[19] Методологія фактчекінгу Ґвара Медіа. URL: https://gwaramedia.com/metodologiya-faktchekingu-perevirka/

ресурсів, а й мінімізувати ризики загроз, що має критичне значення для національної безпеки та стійкості держави.

Зокрема таку роль відіграють наступні нормативно-правові акти, серед яких Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»[20], Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.20 р. № 392/2020[21], Стратегія воєнної безпеки України, затверджена Указом Президента України від 21.03.21 р. № 121/2021[22], Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.21 р. № 447/2021[23], Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.21 р. № 685/2021[24], Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.22 р. № 56/2022[25], а також прийняті з метою їх виконання плани: План реалізації Стратегії кібербезпеки України, введений в дію Указом Президента України від 01.02.22 р. № 37/2022[26], План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, затверджений розпорядженням Кабінету Міністрів України від 30.03.23 р. № 272-р[27], План заходів із реалізації Стратегії забезпечення державної безпеки, затверджений

[20] Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ в.о. Президента України від 01 травня 2014 р. № 449/2014 URL: https://zakon.rada.gov.ua/laws/show/449/2014#Text

[21] Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.20 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

[22] Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 21.03.21 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661

[23] Про рішення Ради безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[24] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

[25] Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України від 16.02.22 р. № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377

[26] План реалізації Стратегії кібербезпеки України : Указ Президента України від 01.02.22 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

[27] Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text

Розпорядженням Кабінету Міністрів України від 18.04.23 р. № 318-р[28], а також відомчі нормативно-правові акти правоохоронних органів України.

Стратегія інформаційної безпеки (затверджена Указом Президента України від 28.12.21 р. № 685/2021) визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, серед яких стосовно впливу сучасних засобів масової інформації, зокрема, було виділено:

– Соціальні мережі як суб'єкти впливу в інформаційному просторі;

– Недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій;

– Обмежені можливості реагувати на дезінформаційні кампанії;

– Несформованість системи стратегічних комунікацій;

– Недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [29].

З метою реалізації поставлених завдань Стратегія інформаційної безпеки України вводить базові поняття, серед окремо виділимо такі:

Інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні;

[28] Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки : Розпорядження Кабінету Міністрів України від 18.04.23 р. № 328-р. URL: https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text

[29] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

Інформаційні заходи оборони держави – сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві;

Стратегічний наратив – спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію.

Виділяють чотири групи суб'єктів протидії дезінформації в Україні:

− органи публічної влади (включаючи представників політичної арени);

− окремі громадяни;

− представники бізнес-сегменту (як правило, середній та великий);

− суб'єкти громадянського суспільства[30].

Центр протидії дезінформації є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106[31]. Центр підпорядкований Раді національної безпеки і оборони України[32]. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Зокрема, до завдань Центру належать:

виявлення та протидія дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі.

[30] Біла книга протидії дезінформації. ГО «Інститут інформаційної безпеки». К., 2022. 62 с. URL: https://postinfosociety.com/bila-knyga-protydiyi-dezinformacziyi/

[31] Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://www.president.gov.ua/documents/1062021-37421.

[32] Центр протидії дезінформації. URL: https://cpd.gov.ua/.

В структурі Міністерства культури та інформаційної політики України в 2021 році було створено і діє Центр стратегічних комунікацій[33]. До основних завдань даного інституту належить:

− комплексний аналіз та оцінка зовнішнього/внутрішнього інформаційного середовища;

− моніторинг відповідних наративів із подальшою оцінкою групи вразливого середовища;

− формування інформаційної гігієни в суспільстві, підвищення рівня обізнаності в питаннях протидії дезінформації;

− підтримка та розвиток урядових публічних комунікацій, в тому числі із проведенням workshop, консультацій, семінарів, нарад, презентацій, інших тематичних заходів;

− формування належних умов для конструктивної взаємодії держави із інституціями громадянського суспільства на шляху до спільної резистенції гібридним загрозам.

Центр стратегічних комунікацій був створений як один з механізмів протидії дезінформації спільними зусиллями держави і громадянського суспільства. Робота Центру сфокусована на комунікаційній протидії зовнішнім загрозам, зокрема – інформаційним атакам. Основними принципами здійснення діяльності Центру є постійна співпраця з громадським сектором, неможливість політичного тиску, відповідальність та відкритість.

Інформаційний імунітет − це здатність ідентифікувати маніпуляцію, фейк, оцінити рівень їх небезпеки і як їм можна запобігти. Для протидії дезінформації необхідно виробити у суспільства інформаційний імунітет, підвищення рівня медіакультури та медіаграмотності суспільства.

Українське суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації, а медіа середовище – бути соціально відповідальним і функціонувати стабільно. За таких умов українське суспільство зможе більш ефективно протистояти державі-агресору та залишатися стійким перед широким спектром загроз, зокрема в інформаційній сфері.

Підвищення рівня медіакультури та медіаграмотності суспільства здійснюватиметься шляхом виконання таких завдань:

– підготовка та проведення просвітницької кампанії з медіаграмотності, що включатиме такі компоненти, як розвиток критичного мислення, навички перевірки фактів і визначення маніпуляційних технік, ознайомлення з найпоширенішими порушеннями прав людини із застосуванням інтернет-технологій тощо;

[33] Центр стратегічних комунікацій. URL: https://spravdi.gov.ua/

– створення сприятливих умов для здійснення діяльності засобів масової інформації;

– створення сприятливих умов для підвищення рівня професійної підготовки медіафахівців;

– удосконалення законодавства у сфері реклами, зокрема щодо лібералізації норм у цій сфері та посилення відповідальності за трансляцію прихованої реклами;

– стимулювання розвитку соціально відповідального бізнесу серед засобів масової інформації.

У 2024 році Google та Jigsaw у партнерстві з Центром протидії дезінформації запустили ініціативу з медіаграмотності в Україні для боротьби з поширенням дезінформації в мережі та підвищення стійкості до поширених методів онлайн-маніпуляцій[34]. Ініціатива, яка використовує підхід під назвою «пребанкінг» (prebunking – дослівно «попереднє розвінчування»), реалізується у співпраці з Moonshot та авторитетними місцевими організаціями й експертами, зокрема Центром протидії дезінформації, Vox Ukraine, StopFake, Детектор Медіа, Суспільне та BBC Media Action.

Пребанкінг – це комунікаційна стратегія, спрямована на підвищення стійкості до дезінформації. Її мета – допомогти аудиторії розпізнавати та протистояти маніпулятивному контенту, підвищуючи стійкість до дезінформації у майбутньому.

Як перший крок ініціативи, партнер з її реалізації компанія Moonshot провела інтерв'ю, щоб дослідити погляди місцевих експертів на дезінформацію та онлайн-безпеку. Moonshot зробив тематичний аналіз даних інтерв'ю, щоб визначити загальні теми дезінформації, методи маніпуляції та аудиторії, які можуть бути вразливішими або стати мішенню дезінформації. Вони надали подальше контекстне підтвердження за допомогою прикладів із соціальних мереж на різних платформах.

Moonshot визначив поточні та нові маніпулятивні наративи, що циркулюють в Україні, та виявив такі три основні техніки маніпуляції:

Астротурфінг (Astroturfing) – ця маніпуляційна тактика передбачає створення видимості суспільних рухів через скоординовану, неавтентичну поведінку, часто з використанням ботів або фейкових акаунтів у соціальних мережах.

Найширше визначення: імітація масової громадської ініціативи для створення ілюзії запиту від суспільства. Астротурфінг використовують як у сфері бізнесу для лобіювання інтересів, так і в галузі піару,

[34] Google та Jigsaw у партнерстві з ЦПД запускають ініціативу з медіаграмотності в Україні (24.07.2024). URL: https://cpd.gov.ua/events/google-ta-jigsaw-u-partnerstvi-z-czpd-zapuskayut-inicziatyvu-z-mediagramotnosti-v-ukrayini/

політики та геополітики (для створення ілюзії масової підтримки чи засудження). Його мета, приміром, – змусити владу дослухатися до «голосу народу», а народ переконати у тому, що певна ідея/особа/концепція «має широку підтримку», тож варто до неї долучитися[35]. В українських соціальних медіа астротурфінг використовується для цілеспрямованого переслідування або штучного пригнічення чи посилення конкретного контенту / наративів. Для цього використовують соціальні мережі, коментарі у пресі, масову розсилку, звернення, петиції (часом інфлюенсери та медіа подають астротурфінг як справжню ініціативу – свідомо чи несвідомо).

Ключовий інструмент сьогоднішнього астротурфінгу – це цифрові технології ботоферм, які імітують масову народну реакцію або ініціативу. Використовується велика кількість ботоферм, що у промислових масштабах займається астротурфінгом. В Україні астротурфінг може мати наступні прояви:

1. Проплачені мітингарі. Приміром, випадки коли на нібито «добровільні мітинги» збирають за гроші маніфестантів. Коли журналісти намагаються їх щось розпитати, ті не можуть відповісти, за що і проти чого вони протестують. Підвид цього астротурфінгу – активисти, які можуть відстоювати свою «громадянську ініціативу» силою.

2. Адмінресурсний астротурфінг. Цей прийом був дуже популярний за СРСР, і уже, менш поширений. Йдеться про ті випадки, коли масовку зганяли з державних підприємств. І виходила гарна картинка велелюдної підтримки влади.

3. Астротурфінг фейкової соціології. Цей метод достатньо простий. Замість того, щоб імітувати «народну підтримку» тієї чи іншої особи або ідеї, можна просто замовити фейкове соціологічне дослідження, що безпідставно видасть потрібну цифру.

Емоційна маніпуляція – провокування сильних емоцій, таких як сум, безнадія, обурення та виснаження, щоб запобігти критичному мисленню щодо теми. В українському контексті емоційні маніпуляції використовуються для посилення психологічного виснаження, спричиненого воєнним конфліктом. Маніпуляції часто стимулюють інтенсивний страх і гнів, щоб загострити соціальні розбіжності, а також для посилення наявної фрустрації щодо українських інституцій і воєнних зусиль.

Підміна контексту – практика вилучення інформації з її оригінального контексту для створення хибного або оманливого наративу. В Україні сфабриковані або маніпулятивні новинні історії поширюють плутанину щодо того, яка інформація або новинні ресурси

[35] Що таке астротурфінг? (25.08.2022). URL: https://uchoose.uacrisis.org/shho-take-astroturfing/

заслуговують на довіру. Дипфейки відомих політиків і військових діячів, згенеровані штучним інтелектом, також націлені на громадян із закликами до капітуляції або відмови від пожертв військовим.

На основі цього дослідження та за експертної підтримки місцевих партнерів було створено три навчальні відео про ці три поширені в Україні методи маніпуляції. Дослідження і рекомендації експертів допомогли сформувати креативну ідею, в основі якої висновки, що найвразливішою аудиторією є молодь і старше покоління, а при оцінюванні інформації люди найбільше довіряють родичам і близьким. Щоб розкрити ці моменти, у відео використовуються реалістичні сімейні діалоги на кухні за участю відомих українських особистостей. Це знайоме середовище відображає місце, де багато сімей ведуть бесіди. Демонструючи розмови про дезінформацію, які охоплюють різні стосунки та вікові групи (батьки-діти, подружжя), відео мають на меті навчити глядачів двом речам: як розпізнавати маніпуляції та як захистити своїх близьких.

Для повноцінної боротьби з поширенням фейків і дезінформації, в тому числі, що загрожує національній безпеці країни, необхідно вдосконалити законодавство. В цьому аспекті корисним є вивчення досвіду інших країн. Відомо, що з проблемою інформаційної безпеки в еру активного розвитку соціальних мереж свого часу зіткнулася провідна європейська країна − Німеччина.

Німеччина є однією з перших країн, яка запровадила санкції на рівні законодавства за поширення неправдивої інформації. Парламентом Німеччини 30 червня 2017 р. був прийнятий Закон «Про вдосконалення правозастосування в соціальних мережах» (Net Enforcement Act (NetzDG)[36]. Це також називається законом Про Facebook. Закон спрямований на боротьбу з дезінформацією (поширення про особу неправдивої інформації, яка принижує її честь та гідність, завдає шкоди діловій репутації) і розпалюванням ненависті в Інтернеті. Закон зобов'язує платформи соціальних мереж з більш ніж 2 мільйонами користувачів встановити прозору процедуру розгляду скарг на незаконний контент і зобов'язує надавати звітність і документацію. Провайдери повинні видаляти «явно незаконний» контент протягом 24 годин, а весь незаконний контент – протягом 7 днів з моменту його публікації, в іншому випадку їм загрожує адміністративний штраф у максимальному розмірі 50 мільйонів євро. Подавачі скарг та користувачі повинні бути негайно проінформовані про прийняті

[36] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 01.09.2017 (Закон про поліпшення правозастосування в соціальних мережах). URL: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

рішення. Віддалений вміст повинен зберігатися щонайменше десять тижнів як доказ, а платформи повинні подавати звіти про прозорість роботи з нелегальним вмістом кожні шість місяців.

ВИСНОВКИ

Проведене дослідження дозволило визначити актуальність проблеми дезінформації у сфері засобів масової інформації в умовах війни в Україні, основні механізми її поширення та дати оцінку сучасним технологіям, що використовуються для протидії інформаційним атакам.

Дезінформація – це потужна зброя гібридної війни, яка активно використовується для підриву довіри до державних інституцій, дестабілізації суспільства та маніпуляції громадською думкою. В умовах війни її вплив стає ще більш руйнівним. Очищення інформаційного простору від фальшивих новин і фейків є обов'язковою умовою подолання війни і перемоги.

Сучасні технології грають вирішальну роль боротьби з дезінформацією.

Використання цифрових технологій дозволить розширити можливості своєчасного повідомлення правоохоронців про правопорушення, розшуку і ідентифікації злочинців, оптимізувати процес розслідування кримінальних правопорушень. Штучний інтелект, автоматизовані системи фактчекінгу та кібербезпека дозволяють виявляти, аналізувати та нейтралізувати інформаційні загрози. Однак ці технології потребують постійного розвитку та адаптації. Для ефективної боротьби з поширенням неправдивої інформації за допомогою інноваційних цифрових технологій необхідно використовувати досвід провідних європейських країн, підвищити роль цифрових інструментів виявлення і протидії дезінформації, в тому числі в роботі правоохоронних органів, із залученням профільних науково-дослідних установ та провідних фахівців в галузі кримінального права адаптувати чинне законодавство до вимог цифрової епохи.

Ефективна протидія дезінформації потребує комплексного підходу. Крім технологічних рішень, важливо розвивати медійну грамотність населення, удосконалювати законодавчу базу та посилювати міжнародне співробітництво у сфері інформаційної безпеки. Україна вже демонструє значні успіхи у боротьбі з дезінформацією, але цей процес має бути постійним та багатошаровим. Важливо поєднувати державні ініціативи, незалежні медіапроекти та активну роль громадянського суспільства. Майбутнє інформаційної безпеки залежить від консолідації зусиль – держави, технологічних компаній, журналістської спільноти та суспільства загалом. Тільки об'єднання цих ресурсів дозволить мінімізувати вплив дезінформації та захистити демократичні цінності.

АНОТАЦІЯ

Стаття присвячена дослідженню проблемам дезінформації в мові сучасних засобів масової інформації та захисту прав людини в інформаційному просторі. В умовах війни дезінформація стає потужним інструментом інформаційно-психологічного впливу, спрямованого на підрив довіри до державних інституцій, маніпуляцію громадською думкою та деморалізацію суспільства. У цій статті розглядаються ключові механізми поширення дезінформації у засобах масової інформації, аналізуються сучасні технології виявлення та протидії фейкам, включаючи штучний інтелект, фактчекінгові платформи та методи кібербезпеки. В роботі приділяється увага проблемі дезінформації в соціальних мережах та інформаційному просторі. Особливу увагу приділено державним ініціативам, міжнародному досвіду та стратегічним підходам до інформаційного захисту України. Зроблено висновок про необхідність комплексного підходу, що поєднує технологічні рішення, законодавчі заходи та розвиток медійної грамотності населення. Автор дійшов висновку, що для ефективної боротьби з поширенням неправдивої інформації за допомогою інноваційних цифрових технологій необхідно використовувати досвід провідних європейських країн, підвищити роль цифрових інструментів виявлення і протидії дезінформації, в тому числі в роботі правоохоронних органів, із залученням профільних науково-дослідних установ та провідних фахівців в галузі кримінального права адаптувати чинне законодавство до вимог цифрової епохи.

Література

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.

2. Нетеса Н. В., Мокляк В. В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право.* 2023. № 3(46). С. 98–107. URL: http://il.ippi.org.ua/article/view/287168.

3. Інформаційна безпека: сучасний стан, проблеми та перспективи: збірник матеріалів Міжнародної науково-практичної конференції. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с. URL: https://politkaf.kpnu.edu.ua/wp-content/uploads/2023/04/zbirnyk-material-konfer.-inf_bezp_2023.pdf

4. Новий алгоритм пошуку Google на основі AI: чого очікувати (29.10.2023). URL: https://livepage.ua/blog/the-new-ai-powered-google-search-what-to-expect.html.

5. Аналітичний звіт «російський інформаційний вплив в Африці». URL: https://cpd.gov.ua/reports/analitychnyj-zvit-rosijskyj-informaczijnyj-vplyv-v-afryczi/.

6. Shevchuk Viktor M. Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*, 2020, 27(2), p.p. 170–183.

7. Велика українська юридична енциклопедія: У 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків: Право, 2018. 952 с.

8. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making (2nd edn, CoE 2008). URL: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

9. Як не стати жертвою шахраїв та ворожої пропаганди: кіберполіція про фактчекінг (02 травня 2024 р). URL: https://cyberpolice.gov.ua/article/yak-ne-staty-zhertvoyu-shaxrayiv-ta-vorozhoyi-propagandy-kiberpolicziya-pro-faktcheking-437/.

10. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України: Законопроект України від 19.04.2023 № 9223 / База даних «Законодавство України» / ВР України. URL: itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk_RIKKEZHmqd699_G6ZH0h9ZmxhEwLZ_ZpXM61T0/.

11. Аналітичний звіт «російський інформаційний вплив в Африці». URL: https://cpd.gov.ua/reports/analitychnyj-zvit-rosijskyj-informaczijnyj-vplyv-v-afryczi/.

12. Посібник для творців контенту для виявлення та протидії російській пропаганді в нових технологіях. (За підтримці Уряду Великої Британії в рамках проекту «Розуміння штучного інтелекту). 2024. URL: https://ai.instingov.org/assets/guide/AI-Guide_uk.pdf

13. Fact-Checking. URL: https://reporterslab.org/fact-checking/

14. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://www.president.gov.ua/documents/1062021-37421.

15. Центр протидії дезінформації. URL: https://cpd.gov.ua/.

16. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 01.09.2017 (Закон про поліпшення правозастосування в соціальних мережах). URL: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

17. Посібник з верифікації. Центр Європейської Журналістики; Асоціація Видавців (УАВПП). 2014. URL: https://verificationhandbook.com/book_ua18.

18. Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи: Практичний посібник. Дніпро : ЛІРА, 2017. 133 с.

19. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1.

20. Ейсмунт В. Інструменти фактчекінгу: як професійно відрізняти брехню від правди. Інститут масової інформації. URL: https://imi.org.ua/articles/instrumenti-faktchekingu-yak-profesiyno-vidriznyati-brehnyu-vid-pravdi-i407.

21. Mantis Analytics. URL: https://mantisanalytics.com/.

22. Фактчек-бот «Перевірка». URL: https://t.me/perevir_bot.

23. Центр протидії дезінформації при РНБО рекомендує новий фактчек-бот «Перевірка» (18.03.2022). URL: https://imi.org.ua/news/tsentr-protydiyi-dezinformatsiyi-pry-rnbo-rekomenduye-novyj-faktchek-bot-perevirka-i44450.

24. Методологія фактчекінгу Ґвара Медіа. URL: https://gwaramedia.com/metodologiya-faktchekingu-perevirka/.

25. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ в.о. Президента України від 01 травня 2014 р. № 449/2014 URL: https://zakon.rada.gov.ua/laws/show/449/2014#Text.

26. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.20 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.

27. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 21.03.21 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661.

28. Про рішення Ради безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

29. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України від 16.02.22 р. № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377.

30. План реалізації Стратегії кібербезпеки України : Указ Президента України від 01.02.22 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text.

31. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text.

32. Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України від 18.04.23 р. № 328-р. URL: https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text.

33. Біла книга протидії дезінформації. ГО «Інститут інформаційної безпеки». К., 2022. 62 с. URL: https://postinfosociety.com/bila-knyga-protydiyi-dezinformacziyi/.

34. Центр стратегічних комунікацій. URL: https://spravdi.gov.ua/.

35. Google та Jigsaw у партнерстві з ЦПД запускають ініціативу з медіаграмотності в Україні (24.07.2024). URL: https://cpd.gov.ua/events/google-ta-jigsaw-u-partnerstvi-z-czpd-zapuskayut-inicziatyvu-z-mediagramotnosti-v-ukrayini/ (дата звернення: 14.02.2025).

36. Criminalistics Means and Methods of Combating Ecocide in the Modern Conditions of Military Threats / V. Shevchuk et al. *Journal of Environmental Law & Policy*. 2024. Т. 04, № 03. С. 82–120. URL: https://doi.org/10.33002/jelp040304 (дата звернення: 14.02.2025).

37. Що таке астротурфінг? (25.08.2022). URL: https://uchoose.uacrisis.org/shho-take-astroturfing (дата звернення: 14.02.2025).

Information about the author:
Nehrebetskyi Vladyslav Valeriiovych,
Candidate of Juridical Sciences,
Researcher
Academician Stashis Scientific Research Institute for the Study of Crime Problems National Ukrainian Academy of Law Sciences
49, Hryhoriia Skovorody street, Kharkiv, 61002, Ukraine,
Associate Professor at the Department of Criminalistics
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody street, Kharkiv, 61024, Ukraine