

ГІБРИДНА ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ

ЯК ПЕРЕМОГТИ
НА ІНФОРМАЦІЙНОМУ
ФРОНТІ



Аналітичний
посібник

2023



ЦЕНТР СТРАТЕГІЧНИХ
КОМУНІКАЦІЙ
ТА ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ



ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА



Швеція
Sverige

Цей посібник розробила команда Центру стратегічних комунікацій та інформаційної безпеки, створеного при Міністерстві культури та інформаційної політики України, спільно з Центром демократії та верховенства права за фінансової підтримки Швеції в межах проєкту «Школа протидії дезінформації».

Інформаційна війна Російської Федерації проти України не менш небезпечна, ніж безпосередні бойові дії. Вона здатна серйозно підірвати єдність українського суспільства, довіру громадян до влади та збройних сил, відносини України з державами-союзниками. Тому для працівників державних структур дуже важливі навички з розпізнавання та протидії російській пропаганді й дезінформації.

Головна мета цього посібника — ознайомлення читачів з основними аспектами протидії російській дезінформації та пропаганді. Для досягнення цієї мети проаналізована інформаційна складова гібридної війни, яку РФ веде проти України; виокремлені основні ознаки та прийоми російської пропаганди й дезінформації; окреслені методи виявлення та адекватного реагування на російську дезінформацію в контексті стратегічних комунікацій, а також запропоновані схеми оцінювання вжитих комунікаційних заходів.

Посібник розроблений для державних службовців і працівників органів місцевого самоврядування. Матеріали будуть корисні керівникам, їхнім заступникам, спеціалістам департаментів, управлінь і відділів, менеджерам з комунікацій, SMM-спеціалістам і всім, хто займається публічною комунікацією від імені державних структур або органів місцевого самоврядування України.

АВТОРИ:

команда Центру стратегічних комунікацій та інформаційної безпеки

ЗА РЕДАКЦІЄЮ

команди Центру демократії та верховенства права

ЦІЛЬОВА АУДИТОРІЯ

Ольга, 27 років,
SMM- спеціалістка
Головного управління
Державної служби
з питань надзвичай-
них ситуацій України
у Тернопільській
області*

Євген, 32 роки,
заступник голови
Миколаївської
обласної державної
адміністрації з питань
диджиталізації

Андрій
Васильович,
65 років, голова
Боромлянської
сільської громади
Сумської області

*Вказані особи та посади є вигаданими

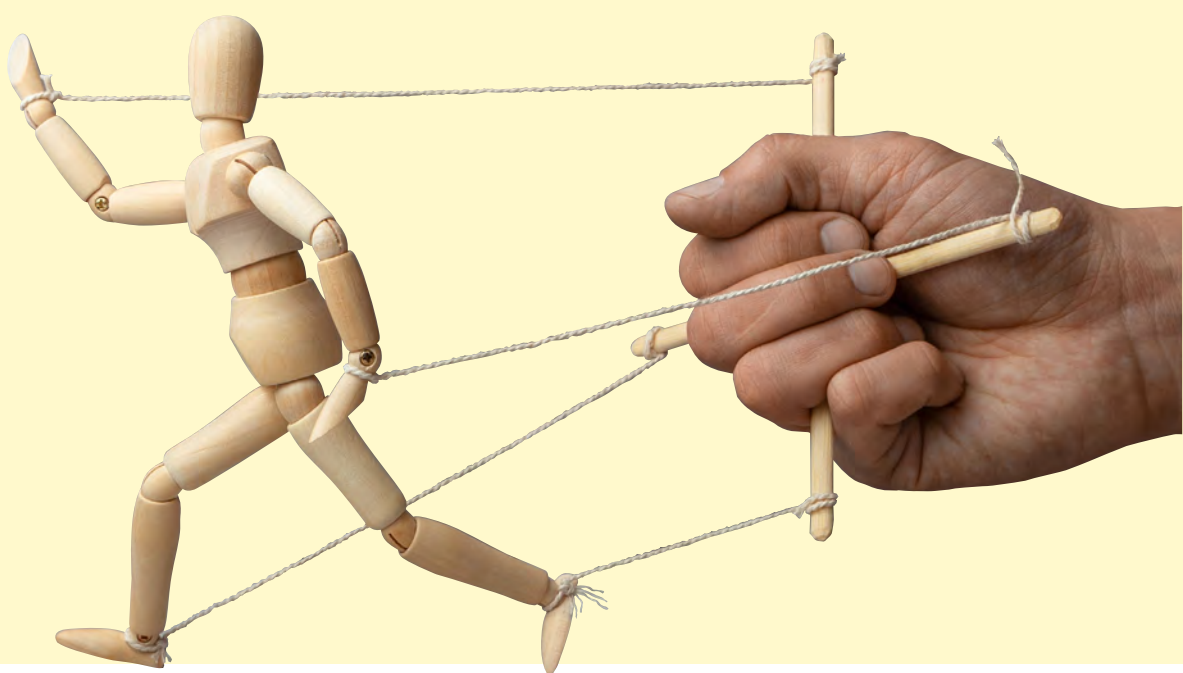
Це посібник підготовлений у межах програми з інституційної розбудови Центру демократії та верховенства права, що здійснюється за фінансової підтримки Швеції.

Думки, висновки чи рекомендації належать авторам/авторкам та упорядникам/упорядницям цього видання і не відображають погляди Уряду Швеції. Відповідальність за вміст публікації несе Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України.



ЗМІСТ

Визначення гібридної та інформаційної війни. Що таке російська пропаганда?	4
Як працює російська пропаганда?	9
Шкідливий вплив російської пропаганди. Навіщо з нею боротися?	16
Як боротися з російською пропагандою?	19
Виявлення	20
Запобігання	26
Стратегічні комунікації	28
Оцінювання вжитих заходів	40
Додатки	45



ВИЗНАЧЕННЯ ГІБРИДНОЇ ТА ІНФОРМАЦІЙНОЇ ВІЙНИ.

ЩО ТАКЕ РОСІЙСЬКА ПРОПАГАНДА?

Концепцію гібридної війни політичні та військові експерти почали активно обговорювати на початку 2000-х років. Утім, вона як явище була поширена ще від початку історії воєн. Однак, попри багатий досвід, накопичений людством у цій сфері, концепція гібридної війни досі не має загальноприйнятого визначення.

У цьому посібнику ми дотримуватимемося такого визначення: **гібридна війна — це воєнна стратегія, що має на меті маскування ролі агресора в конфлікті та передбачає спонсорування заколотів, воєнні дії «під чужим прапором» і широкий спектр невоєнних засобів впливу на противника (економічні, інформаційно-психологічні, кібервійна тощо).**

«Гібридність» (суміш) полягає також у комбінації нетрадиційних (інформаційні та економічні дії) і традиційних (використання збройної сили) методів війни. Гібридна війна потрапляє до так званої «сірої зони» міжнародного права, коли її важко встановити, кваліфікувати й регулювати звичайними правилами (законами і звичаями війни).

ДО ТРАДИЦІЙНИХ МЕТОДІВ ВІЙНИ МОЖНА ВІДНЕСТИ ТАКІ:

- Регулярні збройні сили
- Чітка державна належність
- Дипломатія
- Економічні санкції
- Комплексна логістика
- Розвинені технології
- Домінування вогневої сили
- Дотримання «правил війни»

ДО НЕТРАДИЦІЙНИХ МЕТОДІВ ВІЙНИ НАЛЕЖАТЬ:

- Партизанські методи
- Тероризм
- Підбурювання повстань
- Участь криміналітету
- Кіберінформаційна війна
- Низька інтенсивність
- Використання нерегулярних збройних формувань
- Недотримання «правил війни»¹



Гібридні війни зазвичай не оголошуються, а їх завершення часто не зафіксовано формальними юридичними актами сторін. Узагалі таким конфліктам притаманні дві головні ознаки — розмита межа між війною та миром і високий рівень невизначеності.

Розмитість межі між війною та миром означає, що стає складно виділити поріг війни, коли конфлікт можна окреслити як воєнні дії між державами (суб'єктами конфлікту). Замість того, щоб спрямувати регулярні війська на територію іншої держави, набагато дешевше і, як показує світовий досвід, ефективніше розповсюджувати дезінформацію, засилати незаконні збройні формування, підбурювати місцеву «п'яту колону» (медіа, партії, церкву) і застосовувати економічний шантаж задля досягнення своїх політичних цілей.

Високий рівень невизначеності дає державі, що застосовує гібридні інструменти, можливість приховувати свою причетність до деструктивних дій проти іншої держави. Агресія маскується під інші формати, як-то «спеціальна військова операція» або «допомога братнім республікам Донбасу» тощо.

Своєю чергою державі, проти якої розпочата гібридна агресія, потріб-

но публічно доводити як сам факт зовнішнього нападу на неї, так і причетність до нього конкретної держави-агресора, яка ховається за фасадом недержавних акторів. З огляду на високий рівень невизначеності гібридної війни протистояти гібридним викликам набагато складніше, ніж традиційним військовим загрозам.

Серед інших ознак гібридної війни можна виділити застосування економічних і дипломатичних засобів примусу, кібератаки, інформаційно-психологічні операції. Політолог Євген Магда називає серед її характерних рис використання інформаційної зброї, участь у протистоянні недержавних акторів, **ВИКОРИСТАННЯ ТЕРОРИСТИЧНИХ МЕТОДІВ, НЕХТУВАННЯ ВІЙСЬКОВИМ ПРАВОМ ТА ЕТИКОЮ, ВИКОРИСТАННЯ МЕТОДІВ ЕКОНОМІЧНОГО ТА ПСИХОЛОГІЧНОГО ТИСКУ, ПРОПАГАНДИ ТОЩО².**

¹ Brin Najžer. The Hybrid Age. International Security in the Era of Hybrid Warfare ([Електронний ресурс](#))



² Магда Є. М. Гібридна війна: сутність та структура феномену ([Електронний ресурс](#)).



Ведення гібридної війни дає багато переваг державі, що її застосовує, оскільки дозволяє досягати політичних цілей з мінімальним або взагалі без використання збройної сили, має відносно нижчу ціну та часто уможливорює уникнення відповідальності перед світовою спільнотою за воєнні злочини й інші порушення норм міжнародного права. У гібридній війні можна виділити чотири ключові сфери — економіку, зброю, недержавних акторів, інформацію.

■ **ЕКОНОМІКА.** Створення економічних проблем через вплив на ринки та перешкодження зв'язкам країни-жертви з партнерами. Наприклад, штучне завищення Росією цін на газ у Європі взимку 2021–2022 рр.

■ **ЗБРОЯ ТА ТАЄМНІ ОПЕРАЦІЇ.** Цільове постачання зброї учаснику чи учасникам конфлікту з метою його затягування, повалення влади або дестабілізації регіону. Широка роль спеціальних служб і таємних операцій. Наприклад, постачання Іраном зброї ісламістському угрупованню «Хезболла» у Лівані або постачання зброї Росією сирійському диктатору Башару Асаду.

■ **НЕДЕРЖАВНІ АКТОРИ.** Використання проксіформувань замість сил регулярної армії. Наприклад, участь російської ПВК «Ліга» (раніше — «Вагнер») у конфліктах у Латинській Америці, Африці та на Близькому Сході.

■ **ІНФОРМАЦІЯ.** Створення внутрішніх суспільних суперечок через пропаганду, неправдиві новини, дезінформацію. Наприклад, інформаційна діяльність ІДІЛу з вербування нових учасників терористичного руху.

Саме інформаційна складова — найважливіший і найпотужніший елемент гібридної війни: з нею найскладніше боротися і водночас вона приносить бажані результати без військового втручання. Цей посібник спрямований на вироблення підходів для боротьби з головними інструментами інформаційної війни РФ — пропагандою, дезінформацією та маніпуляціями.

Інформаційна війна передбачає застосування засобів інформаційно-



го впливу, які включають потенційно деструктивні форми комунікації, що застосовуються іноземними державами або їхніми представниками. Вони передбачають навмисне втручання у внутрішні справи держави з метою підризу довіри між владою та громадянами. Інформаційна війна використовується для просування інтересів іноземної держави через експлуатацію вразливостей у суспільстві з метою його поляризації та дестабілізації³.

Росія активно застосовує гібридну війну, особливо її інформаційну складову, проти західних держав і своїх сусідів з початку 2000-х років. Доктринально бачення гібридної війни російським військово-політичним керівництвом сформувалося у



2013 році, коли начальник Генштабу Збройних Сил РФ Валерій Герасимов оприлюднив статтю «Цінність науки в передбаченні», ідеї якої надалі отримали назву «доктрина Герасимова». У статті пропонується новий погляд на ведення війни. Головний принцип «доктрини Герасимова» — використання нетрадиційних військових методів (економічний тиск, таємна дипломатія, інформаційна війна, захоплення сепаратизму) замість прямого вторгнення на територію іншої держави задля досягнення основних політичних цілей. Ця доктрина застосовується проти України з 2014 року⁴.

Варто зауважити, що російська воєнна доктрина розглядає гібридну війну не так, як це роблять інші держави.

Для РФ гібридна війна — це не набір певних інструментів, а тип конфлікту, у якому всі засоби, включаючи військові операції, є складовими єдиної централізованої інформаційної кампанії. Тобто Росія воює також за свідомість противника.

Російські аналітики бачать мету гібридної війни як отримання здатності визначати довгострокове управління та стратегічну орієнтацію іншої держави. На думку РФ, держави-переможниці в гібридних війнах успішно нав'язують переможеним свій світогляд, цінності, інтереси та розуміння «справедливого» розподілу ресурсів. Держави-переможці тоді отримують владу і, з погляду Росії, право визначати майбутнє іншої країни⁵.

Зважаючи на мету гібридної війни, яку вела Росія, основним методом досягнення політичних цілей виступають інформаційно-психологічні операції, які складаються з пропаганди, поширення неправдивих новин і дезінформації.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА ОПЕРАЦІЯ (ІПСО) —

комплекс заходів, спрямованих на формування в широкої (чи цільової) ворожої аудиторії переконань і настроїв, які послаблюють її опірність і тим самим полегшують досягнення воєнних цілей. Зазвичай ІПСО чинять психологічний тиск на суспільство, поширюють панічні настрої та підривають довіру до державних інститутів.



³ Countering information influence activities. A handbook for communicators
([Електронний ресурс](#))



⁴ Molly K. McKew. The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you
([Електронний ресурс](#))



⁵ Mason Clark. Russian Hybrid Warfare ([Електронний ресурс](#))



■ Найяскравішим прикладом російської ІПсО на початку повномасштабної війни у 2022 році стала операція з масовим малюванням міток і залишенням незрозумілих пристроїв на об'єктах цивільної інфраструктури України. Для цього залучалися в основному українські громадяни: російські куратори від спецслужб знаходили їх у месенджерах і пропонували грошову винагороду. Одночасно російські дезінформатори стали просувати наратив про те, що ці мітки та пристрої — засоби наведення авіаційних, ракетних й артилерійських ударів по території України, а також нібито те, що вони допомагають російським військам краще орієнтуватися на місцевості.

Головною метою цієї операції було посіяти паніку та хаос серед цивільного населення України. Також російські пропагандисти мали на меті показати, що в Україні достатньо людей, які готові стати зрадниками за гроші, і відвернути увагу органів правопорядку та населення від справжніх російських диверсантів і колаборантів, що дозволило їм вільніше займатися своєю підривною діяльністю.

■ Чимало зусиль російські спеціалісти з ІПсО докладають на тимчасово окупованих територіях України. Так, пропагандисти просували наратив про те, що відключення мобільного зв'язку на Херсонщині — справа рук української влади, таким чином формуючи в населення, яке там залишилося, відчуття того, що «Україна їх покинула».

■ Російські ІПсО-підрозділи використовують застарілі й традиційні методи пропаганди на тимчасово окупованих територіях: опитування населення для оцінювання настроїв, інформаційний супровід постановочних «гуманітарних акцій», спілкування з місцевими громадянами за технологіями «сарафанного радіо», роздачу інформаційних матеріалів на кшталт листівок або газет.

Одночасно спільно зі співробітниками ФСБ/ГРУ проводиться вербування наших громадян для подальшої співпраці та участі в колаборантській діяльності. Зрадники отримують статус «позаштатного співробітника» й заробітну плату близько 70 тис. рублів. Ці колаборанти організовують та особисто беруть участь у пропагандистських акціях, поширюють проросійський контент у соціальних мережах та інших каналах комунікації тощо.

■ Ще одним прикладом російської ІПсО, спрямованої на все населення України, був злам хакерами новинної стрічки телеканалу «Україна 24» та розміщення там неправдивої заяви нібито Президента України Володимира Зеленського про капітуляцію нашої держави. Такі операції мають на меті деморалізувати населення України та підірвати його довіру до влади.

■ Для деморалізації воїнів Збройних Сил України ворог використовує різні ІПсО-технології. Рідним солдатів й офіцерів телефонують, щоб повідомити неправдиву інформацію про стан і місце перебування військових.

■ Самим бійцям ЗСУ також часто надходять смс-повідомлення з погрозами, що росіяни нібито знають їх конкретне місце перебування, персональні дані тощо.



ЯК ПРАЦЮЄ РОСІЙСЬКА ПРОПАГАНДА?

Російська пропаганда почала набирати рис, які їй притаманні сьогодні, після «Помаранчевої революції» 2004 року в Україні – саме тоді Кремль мобілізував всі пропагандистські можливості не проти якихось окремих персоналій чи об'єктів, а проти всієї держави. Її ефективність була відпрацьована в ході російсько-грузинської війни 2008 року і радикалізувалася після незаконної анексії Криму та агресії на сході України.

24 лютого 2022 року активізувало подальше перетворення російської пропаганди, внаслідок чого вона стала ще більш агресивною, реваншистською та радикальною.

Цільовою аудиторією ІПсО Росії в Україні виступає проросійське населення з різних регіонів України з фокусом на російськомовних громадянах, держслужбовцях, інтелектуальній еліті й людях старшого віку.

На цей момент модель російської пропаганди характеризується чотирма відмінними рисами:

- великий обсяг і мультиканальність;
- швидкість, безперервність і повторюваність;
- відірваність від об'єктивної реальності;
- відсутність послідовності;
- наративізація.



ВЕЛИКИЙ ОБСЯГ І МУЛЬТИКАНАЛЬНІСТЬ

Особливість людської психології — ставати на сторону більшої, дотримуватися найпопулярнішої точки зору, навіть якщо вона хибна. Кремль вдало використовує цю слабкість. Для цього він розвинув масштабну мережу, яка працює на пропаганду: ТБ-канали, інформаційні агентства, онлайн-видання, соціальні мережі та навіть «фабрики тролів»* і «ботоферми»**. Множинність каналів, через які передається інформація, а також її великий обсяг роблять основні наративи пропаганди більш переконливими для потенційного споживача.

RT (раніше Russia Today) — один з основних постачальників мультимедійних новин у Росії. З бюджетом понад 300 млн дол. на рік медіахолдинг мовить англійською, французькою, німецькою, іспанською, російською та кількома східноєвропейськими мовами. Канал особливо популярний в інтернеті, де має понад мільярд переглядів сторінок. Якщо цифра правдива, то це най-

популярніше джерело новин в інтернеті. Окрім того, існують десятки проксісайтів новин, які транслюють російську пропаганду, але їх пов'язаність з Росією приховується чи применшується.

26 лютого 2022 року Служба безпеки України викрила та знешкодила російську «ботоферму» на 7 тис. акаунтів, що займалася пропагандою війни. У 2021 році служба виявила «ботоферму», яка управлялася з РФ і була направлена на зрив вакцинації від коронавірусу в Україні. Злочинна мережа налічувала більше ніж 5 тис. акаунтів.

Служба безпеки України оприлюднила список телеграм-каналів, які розповсюджують російську пропаганду в Україні. Серед них такі відомі канали, як «Легітимний», «Резидент» тощо.

Також російські пропагандисти вже після початку повномасштабної війни створили чимало нових телеграм-каналів для тимчасово окупованих територій (Херсон, Мелітополь, Бердянськ тощо) і міст, де велися чи ведуться бойові дії (Харків, Чернігів), через які проводять свої ІПсО та активно розповсюджують дезінформацію та фейки.

ШВИДКІСТЬ, БЕЗПЕРЕРВНІСТЬ І ПОВТОРЮВАНІСТЬ

Дуже часто російські новинні сайти та ТБ-канали оперативно висвітлюють певні події. Це стається тому, що такі новини — фейки, вигадані завчасно, або маніпуляція, прописана в методичці від уряду. Утім, потенційний споживач більш схильний вірити тому, що почув найперше і натрапив в інших джерелах. Тому навіть якщо читач побачить пізніше правдиву новину, то буде

дотримуватися думки, яку почув раніше кілька разів.

Такий феномен пояснюється в психології різновидом когнітивного упередження — «підтверджувальним упередженням».

ПІДТВЕРДЖУВАЛЬНЕ УПЕРЕДЖЕННЯ — це тенденція шукати або інтерпретувати інформацію таким чином, щоб вона підтверджувала власні переконання або гіпотези, а також схильність ігнорувати інформацію, що суперечить переконанню.⁷



Тенденцію вірити інформації, яка підтверджує вже наявні переконання, підкріпило одне із соціологічних опитувань у Росії. 89 % росіян вірять, що метою «спеціальної військової операції» є захист мирного населення Донбасу, запобігання нападу на Росію та «денацифікація» України.

Також підтверджувальне упередження проявляється в тому, що нібито західні країни підштовхують Україну до війни, незважаючи на те, що саме Росія розпочала неспровоковане та невинуватене вторгнення на українську територію.

Російські пропагандисти часто першими опиняються на місці подій, що створює ілюзію «ексклюзивної інформації від першоджерела». Зокрема, це буває після [обстрілів](#) і [вибухів](#), що нагтовхує на серйозні підозри в тому, що частина подібних новин — просто зрежисовані вистави.

Найяскравішим прикладом безперервності та повторюваності може слугувати російський пропагандистський міф про те, що нібито «ЗСУ вісім років бомблять Донбас і вбивають дітей». За вісім років цей наратив дуже сильно вкоринився в головах

росіян і зараз активно використовується владою РФ для виправдання повномасштабного вторгнення в Україну — так званої «спеціальної військової операції» та всіх воєнних злочинів, які чинить російська армія на території нашої держави. Вони апелюють до принципу «око за око, зуб за зуб». Російські пропагандисти подають це як «помсту за восьмирічні обстріли Донбасу».

* **Фабрики тролів** — це сукупність певної категорії користувачів соціальних мереж і різних форумів, які за гроші лишають дописи та коментарі під новинами інтернет-видань або на інших ресурсах у мережі з метою розповсюдження дезінформації та пропаганди.

** **Ботоферми** — це компанії, які створюють несправжніх користувачів соцмереж у великих масштабах і від їхнього імені пишуть тисячі коментарів, зазвичай негативних і націлених на дискредитацію особи, події чи розпалювання ненависті.

⁶Christopher Paul, Miriam Matthews. The Russian «Firehose of Falsehood» Propaganda Model ([Електронний ресурс](#))



⁷Joshua Klayman and Young-Won Ha. Confirmation, Disconfirmation, and Information in Hypothesis Testing ([Електронний ресурс](#))



3

ВІДІРВАНІСТЬ ВІД ОБ'ЄКТИВНОЇ РЕАЛЬНОСТІ

Російська пропаганда дуже часто поширює дезінформацію та фейки. РФ не потрібно маніпулювати якимись фактами, якщо їх можна просто вигадати, оформивши в новину від надійного джерела.

Прикладами відірваності від об'єктивної реальності можуть слугувати російські дезінформаційні наративи про «бойові наркотики, які вживають військовослужбовці ЗСУ для без-

страшності», «підготовку загонів сатаністів для війни з Росією», «комарів і перелітних птахів, що цілеспрямовано переносять небезпечні хвороби, адаптовані під слов'янський етнос у біолабораторіях України». Як, власне, і існування біолабораторій загалом.

Серед інших «геніальних» витворів російської пропаганди можна відзначити фейки про нібито канонізацію Православною церквою України Степана Бандери, який був греко-католиком, і створення на базі 80 бригади десантно-штурмових військ ЗСУ окремого гей-батальйону «Блакитний смерч» з представників ЛГБТ-спільноти.

4

ВІДСУТНІСТЬ ПОСЛІДОВНОСТІ

Найбільш парадоксальною характеристикою російської пропаганди є її непослідовність. Різні канали комунікації можуть транслювати різну інформацію стосовно однієї і тієї ж теми. Понад те, часто одне й те саме російське джерело змінює свій погляд або меседж. Однак це не викликає недовіри споживача.

Яскравим прикладом непослідовності пропагандистів стали дуже різні та строкаті меседжі про вибух російського складу боєприпасів у Новій Каховці 11 липня 2022 року.

5

НАРАТИВІЗАЦІЯ

Найбільш парадоксальною характеристикою російської пропаганди є її непослідовність. Різні канали комунікації можуть транслювати різну інформацію стосовно однієї і тієї ж теми. Понад те, часто одне й те саме російське джерело змінює свій погляд або меседж. Однак це не викликає недовіри споживача. Російська пропаганда часто непослідовна у своїх меседжах, однак загальні наративи залишаються сталими. Наприклад, в історії про бабусю з червоним прапором, яку активно розганяла російська про-

паганда і яку Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України ефективно розвінчав, загальний наратив був один — показати, що населення України на боці російських загарбників. Утім, окремі меседжі суперечили одне одному: бабуся була то з Київщини, то з Донеччини. Після оприлюднення інтерв'ю цієї бабусі, де вона спростувала свою прихильність до Росії, у ворожій пропаганді з'явилося безліч різноманітних меседжів: від того, що бабусю викрала Служба безпеки України, до того, що вона українська націоналістка.



Часто російська пропаганда одночасно підтримує два меседжі, що конфліктують між собою і поляризують суспільство. Так, під час піка коронакризи та розгортання кампанії з вакцинації в Україні російські боти та тролі в соціальних мережах висували уряду України два протилежні за змістом звинувачення: а) проведення примусової вакцинації, яка нібито шкідлива для здоров'я; і б) недостатні темпи проведення вакцинації населення.

Росія та її пропаганда поляризують не лише українське суспільство, а й населення країн Європейського Союзу. Так, у Німеччині росіяни відверто підтримують як ультраправу партію «AfD», так і ультраліву «Die Linke», які є ідеологічними антагоністами. Проте представники обох партій системно транслиують наративи російської пропаганди і виправдовують російську агресію проти України. Яскравими прикладами є [промова співголови парламентської фракції «AfD» Аліс Вайдель у Бундестагу та виступи експівголови партії «Die Linke» і депутатки Бундестагу Сари Вагенкнехт](#).

Російська пропаганда реалізується через так званий «ланцюг дезінформації». Він складається з чотирьох категорій — **КЕРІВНИЦТВО, ПРОКСІОРГАНИ, КАНАЛИ ПОШИРЕННЯ ТА СПОЖИВАЧІ**.

ДО ПЕРШОЇ КАТЕГОРІЇ — КЕРІВНИЦТВА — належить політична та військова верхівка РФ: президент Володимир Путін, начальник Генштабу Збройних Сил РФ Валерій Герасимов, очільник Міністерства закордонних справ Сергій Лавров та інші високопосадовці й офіційні особи. Саме політично-військовий істеблшмент Росії — основне джерело дезінформації не лише на внутрішню аудиторію, а й міжнародну спільноту. Маніпуляції, які озвучує постійний

представник РФ при ООН Василь Небензя під час засідань Ради Безпеки ООН, заяви Володимира Путіна під час телефонних розмов зі світовими лідерами, інтерв'ю Сергія Лаврова — усе це слугує фактично першоджерелом російської пропаганди.

ДРУГА КАТЕГОРІЯ — ПРОКСІОРГАНИ, до яких належать організації, що втілюють російські пропагандистські інформаційні кампанії. Такі організації за залежністю від російського уряду поділяються на три типи:

- 1 Органи, афілійовані з вищим щаблем російської влади, такі як ФСБ та ГРУ МО РФ;
- 2 Організації, які формально не пов'язані з урядом, однак фактично ним керуються, оскільки фінансуються з державного бюджету. Яскравим прикладом слугує RT (раніше Russia Today) — російська державна телекомпанія, інформаційне агентство «Sputnik»;
- 3 Органи, зв'язок яких з російським урядом прихований. Сюди належить «Агентство інтернет-досліджень», також відоме як «санкт-петербурзька фабрика тролів». Агентство розташовувалось у Санкт-Петербурзі й просуває дезінформацію різними каналами комунікації, переважно в соціальних мережах.

ОСТАННЯ КАТЕГОРІЯ — СПОЖИВАЧІ. Сюди належать різні категорії населення різних держав залежно від цільової аудиторії, на яку спрямована інформаційна кампанія РФ. Це можуть бути звичайні громадяни, бізнесмени, політики та лідери громадської думки.

ПРАКТИЧНІ МЕХАНІЗМИ російської пропаганди налічують безліч прямих і непрямих форм впливу. Більшість експертів погоджується, що їх умовно можна поділити на **«ПОЗИТИВНІ»** (створення позитивного іміджу влади в РФ) і **«НЕГАТИВНІ»** (поширення фейків, маніпулювання фактами). Що ж до **КОНТЕНТУ, ТО ЙОГО КЛАСИФІКУЮТЬ ЗА ТРЬОМА КАТЕГОРІЯМИ — ДЕЗОРІЄНТУВАЛЬНИЙ, ОХОРОННИЙ ТА АГРЕСИВНИЙ.**

Головною метою **ДЕЗОРІЄНТУВАЛЬНОГО** контенту постає знищення концепту правди: такий контент намагається переконати, що об'єктивної істини не існує, а тому жодні інституції, особливо владні, не варті довіри. На внутрішньому ринку **ОХОРОННИЙ КОНТЕНТ** прагне створити ілюзію, що чинна російська влада захищає власний народ і їй немає жодних політичних альтернатив.

Тим часом зовнішній вектор охоронного контенту, зокрема, український, передбачає дискредитацію чинного істеблішменту. Давно знайомі нам наративи про те, що «агресивний Захід» намагається знищити «мирну та квітучу Росію», належать до цього типу контенту.

АГРЕСИВНИЙ контент нагадує **ОХОРОННИЙ** за структурою, однак містить сильні емоційно забарвлені меседжі: потрібно захищати «руський мир» від рук «американського захватчика», а Україну витягувати з лап «фашистської хунти», «соросят», «демпартии», «Гейропы» і подібне.

Утім, починаючи з 2020 року, ці категорії контенту змінилися й набрали більш агресивної форми. Причина — російських споживачів перестало задовольняти заповнення ефіру телеканалів українською та американською тематикою, у них почали виникати претензії з приводу утисків прав та свобод, занедбаного стану медичної та соціальної сфер, на фоні ковідної кризи знижувався рейтинг режиму. Це призвело до того, що **ДЕЗОРІЄНТУВАЛЬНИЙ** підхід усе ж знайшов істину — вона в устах державного керівництва. Вірити можна лише владі й більше нікому⁸.

ПІСЛЯ 24 ЛЮТОГО 2022 РОКУ ОХОРОННИЙ ТА АГРЕСИВНИЙ КОНТЕНТ об'єдналися з однією метою — виправдати неспровоковане вторгнення Росії в Україну. Тепер російська пропаганда підвищує градус, демонізуючи Захід, звинувачуючи в усьому Україну та наголошуючи на потребі захисту російських цінностей. Після 24 лютого російська пропаганда почала просувати три ключові наративи, які певним чином супроводжують військове вторгнення в Україну. Перший з них — **ВІД САНК-**





ЦІЙ СТРАЖДАЮТЬ ПРОСТІ РОСІЯНИ, ЯКІ НЕ РОЗУМІЮТЬ, ЩО ВІДБУВАЄТЬСЯ. Таким чином, Кремль, фокусуючи увагу на «наївних і ні в чому не винних» громадянах РФ, провокує дебати у західних країнах щодо доцільності санкцій.

Другий — **ВТОРГНЕННЯ В УКРАЇНУ — ЦЕ ВІЙСЬКОВА ОПЕРАЦІЯ, А НЕ ВІЙНА.** Росія відмовляється називати те, що вона робить в Україні, війною. Натомість Кремль використовує термін «спеціальна військова операція». Такі ж наративи можна помітити в деяких західних медіа, які замість слова «війна» послідовно використовують терміни «криза» або «конфлікт». Таким чином, Кремль намагається уникнути відповідальності за злочини агресії відповідно до міжнародного права та виправдати загарбницьку війну в очах власного населення.

І нарешті третій наратив — **УКРАЇНОФОБІЯ.** Російські медіа змальо-

вують українських військових як неонацистів і воєнних злочинців, а українських біженців — як невдячних й агресивних «гастарбайтерів». Окрім того, російська пропаганда принижує історію та культурне надбання України, ставлячи під сумнів «справжність» її державності. Таким чином, Кремль намагається переконати Захід у тому, що Україні не варто допомагати, оскільки вона не є суверенною державою, а її населення — цивілізованим народом⁹.

⁸ Ксения Кириллова. Российская пропаганда запускает новый этап мобилизации ([Електронний ресурс](#))



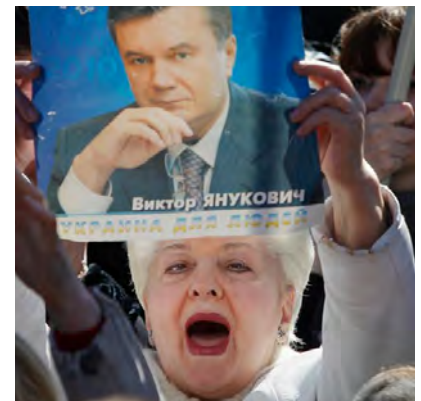
⁹ Anna Romandash. Russian propaganda is affecting you more than you think ([Електронний ресурс](#))



ШКІДЛИВИЙ ВПЛИВ РОСІЙСЬКОЇ ПРОПАГАНДИ.

НАВІЩО З НЕЮ БОРОТИСЯ?

Російська пропаганда, зважаючи на цілі та засоби їх досягнення, негативно впливає на суспільство за кордоном. Основним результатом її впливу стає **ДЕСТАБІЛІЗАЦІЯ СИТУАЦІЇ** всередині іншої держави. Вона досягається передусім шляхом **ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТЕЙ**, наявних у суспільстві. Наприклад, постійне підживлення дебатів з приводу двох державних мов в Україні в результаті **ПІДРИВАЄ ЗГУРТОВАНІСТЬ** українського суспільства та **ПРОВІДИТЬ МЕЖУ** між країномовними та російськомовними.



Наратив російської пропаганди про «утиски російськомовних людей в Україні» — один з найстаріших і системно поширюється ще з початку 1990-х років. Яскравим прикладом є діяльність проросійського активіста та експрезидента Криму Юрія Мешкова у 1990-х роках, коли відбулася по суті перша спроба відділити Крим від України й приєднати до Росії, яка, на щастя, провалилася.

Соціально-політична технологія штучного розколу України за мовною та регіональною ознаками активно використовувалася під час резонансних президентських виборів 2004–2005 рр., а також протягом усього президентства Віктора Ющенка. Достатньо згадати листівку про «три сорти українців», авторство якої приписують російському політтехнологу Віктору Януковича Тимофію Сергєйцеву. Це зображення активно поширювалося в Україні протягом виборчої кампанії 2004–2005 рр.

Чергового поштовху цій хвилі пропаганди надало ухвалення у 2017 році нового Закону України «Про освіту», визнання Конституційним Судом України у 2018 році «мовного закону Ківалова-Колесніченка» (Закону України «Про засади державної мовної політики») неконституційним, а також ухвалення у 2019 році Закону України «Про

забезпечення функціонування української мови як державної». Росіяни продовжили розвивати цей наратив уже у 2022 році під час повномасштабної війни, коли Верховна Рада України ухвалила закони, [що обмежують поширення російської музики в Україні](#) та [забороняють ввезення книг з РФ та Білорусі](#).

Абсурдність цієї пропагандистської теми добре продемонструвало [соціологічне опитування, проведене у травні 2022 року Київським міжнародним інститутом соціології](#). 90 % російськомовних українців і 85 % етнічних росіян, що є громадянами України, заявили про відсутність жодних утисків російської мови на території нашої держави.



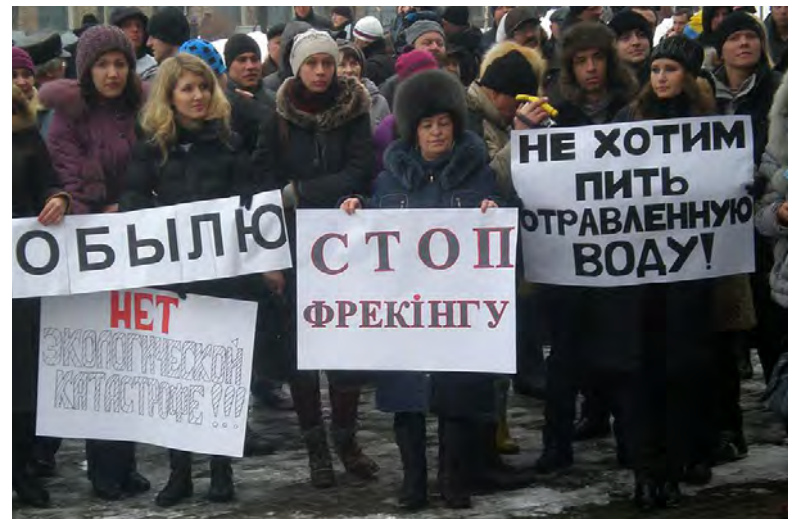
Інший спосіб дестабілізації — ПІДРИВ ДОВІРИ ДО ДЕРЖАВНИХ ІНСТИТУЦІЙ І СИЛОВИХ СТРУКТУР.

Поширення фейків і дезінформації про діяльність державних органів і створення образу влади, що бреше, сприяє руйнуванню легітимності уряду в очах населення. Такий сценарій був реалізований на території так званих «ДНР» і «ЛНР», що призвело до сильних антиукраїнських настроїв у регіоні під час подій 2014 року. Російські інформаційні агентства фактично з другої половини 2000-х років поширювали наратив про те, що влада в Києві експлуатує поклади корисних копалин і вичавлює максимальну економічну вигоду з підприємств Донбасу, натомість штучно підтримує рівень життя мешканців регіону на низькому рівні. Таким чином, у головах частини населення Донецької та Луганської областей вкорінилося уявлення про те, що вони «годуєть усю Україну», однак самі живуть бідно, тому що уряд їх визискує.

Яскравий приклад — масові протести у 2013 році проти видобутку сланцевого газу, що пройшли в містах Донецької області. За даними журналіста-розслідувача Христо Грозєва, ці протести фінансувалися російськими спецслужбами за підтримки тодішнього генерального консула РФ у Харкові Віктора Мокіна. Політичним ядром «антисланцевого» руху були представники Комуністичної партії України та структури Віктора Медведчука «Український вибір». Також були активно залучені представники місцевих екологічних організацій. Очевидно, що РФ і «Газпрому» було вкрай не вигідне різке зростання видобутку газу в Україні, ще й за допомогою західних компаній. Цікаво, що ті ж самі протестні групи були використані навесні

2014 року для сприяння тимчасовій окупації Слов'янська та проведенню незаконного «референдуму» про незалежність так званої «ДНР»¹⁰.

Тема «страшної екологічної небезпеки» під час видобутку сланцевого газу використовувалася російськими пропагандистами і після 2013 року. Протести в Харківській та Донецькій області тривали аж до початку повномасштабного вторгнення у 2022 році. Людей відверто залякували, пропаганда будувалася переважно на емоціях^{11,12,13}.



¹⁰ Захоплення Слов'янська починалося як протести проти сланцевого газу?
([Електронний ресурс](#))



¹¹ Екологія чи державна зрада?
([Електронний ресурс](#))

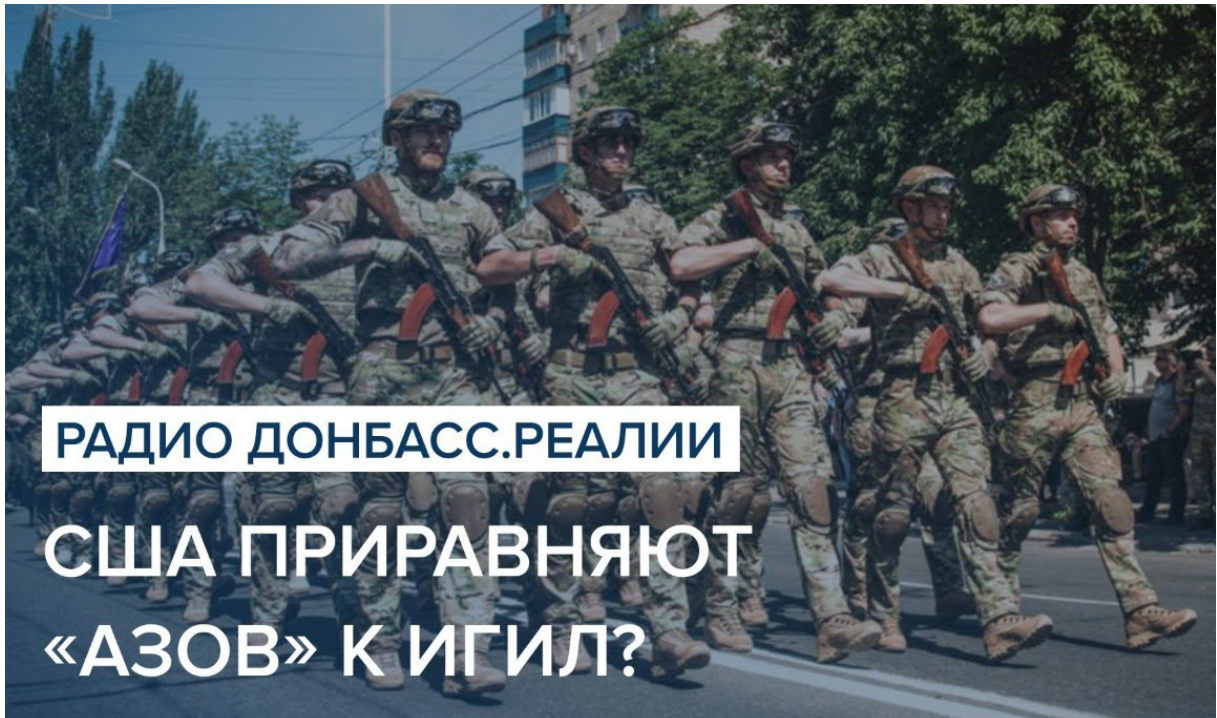


¹² Жителі Мерефи на п'ять годин перекрили трасу на знак протесту проти видобування сланцевого газу
([Електронний ресурс](#))



¹³ «Газові» протести на Донбасі і навіяні фобії
([Електронний ресурс](#))





РАДИО ДОНБАСС.РЕАЛІИ

США ПРИРАВНЯЮТ «АЗОВ» К ИГИЛ?

Росіяни також постійно й системно поширюють дезінформаційний наратив про нібито звірства та війнні злочини ЗСУ й Національної гвардії, роблячи особливий акцент на «терористичному» і «неонацистському» полку «Азов», що має на меті посіяти недовіру українського суспільства до діяльності власних силових структур і зменшити їх підтримку суспільством. Такі наративи особливо активно поширюються на тимчасово окупованих територіях через підконтрольні росіянам медіа та телеграм-канали, щоб і надалі підривати довіру до української влади, здобути лояльність населення, що там залишилося, і ускладнити майбутній процес реінтеграції.

Російська пропаганда вигадала термін «нацбати» для протиставлення окремих військових формувань решті сил оборони. Активно розкручуються пропагандистські меседжі про «невелику купку бойовиків-націоналістів, що використовуються як загороджувальні загони проти ЗСУ, Національної гвардії тощо». Хоча загальновідомо,

що всі добровольчі формування в Україні вже давно інтегровані в офіційні державні силові структури.

Усі ці прояви та засоби російської пропаганди вказують на одну з фундаментальних цілей інформаційної війни, яку веде Росія, — контроль над населенням іншої держави. Стратегія інформаційної безпеки України, зважаючи на вплив російської пропаганди та дезінформації, **ВИЗНАЧАЄ ІНФОРМАЦІЙНИЙ ВПЛИВ РОСІЇ ЯК ЗАГРОЗУ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ.**

САМЕ ТОМУ БОРОТЬБА ТА ЗАПОБІГАННЯ ІПСО РОСІЇ НА ТЕРИТОРІЇ УКРАЇНИ НАДЗВИЧАЙНО ВАЖЛИВІ ДЛЯ ЇЇ СУВЕРЕНІТЕТУ, ефективної діяльності державних структур і гармонійного існування українського суспільства.

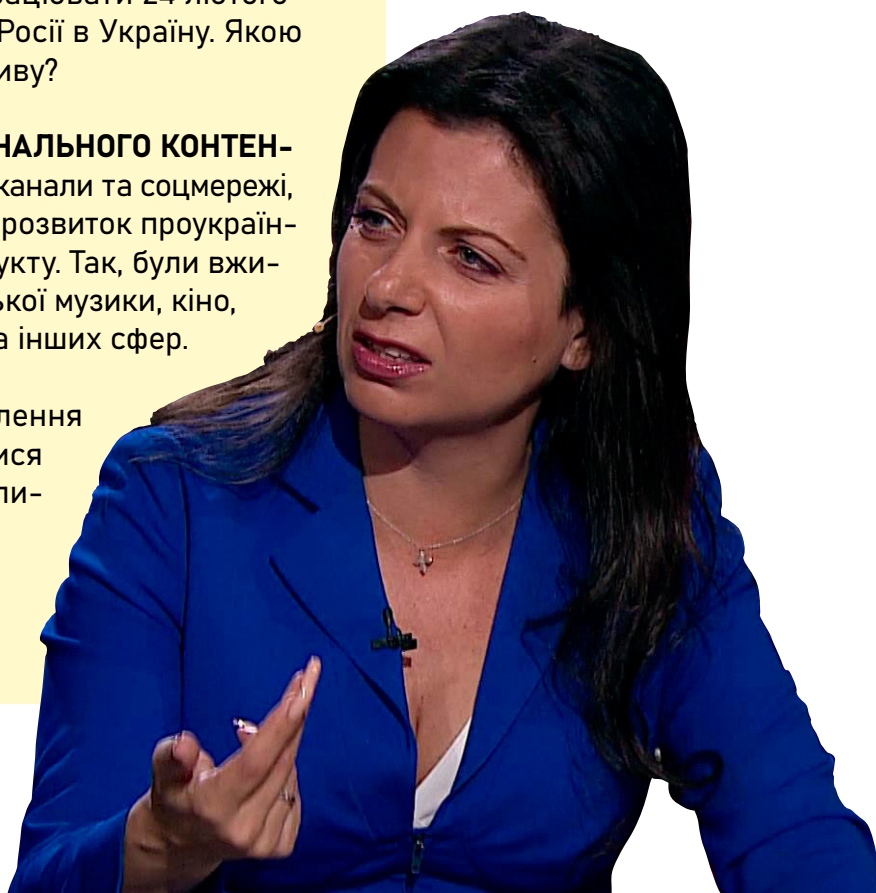


ЯК БОРОТИСЯ З РОСІЙСЬКОЮ ПРОПАГАНДОЮ?

Центр стратегічних комунікацій та інформаційної безпеки пропонує дорожню карту боротьби з російською пропагандою, дезінформацією та маніпуляціями. З метою кращого розуміння об'єкта аналізу розпочнемо з визначення дезінформації, мізінформації, маніпуляції та фейків.

На державному рівні боротьба з ворожим інформаційним впливом має кілька етапів:

- 1 БЛОКУВАННЯ ДОСТУПУ ВОРОЖИХ КАНАЛІВ КОМУНІКАЦІЇ.** Україна пішла цим шляхом у 2014 році, заборонивши трансляцію у своїх кабельних мережах російських телеканалів. Ще через три роки, у 2017 році, поза законом опинилися також російські пошуковики (Яндекс.ру) та соцмережі (Вконтакте, Однокласники). У 2021 році закрито і пул телеканалів Віктора Медведчука, які існували на російські гроші та працювали в унісон з російською пропагандою. Досвід показав ефективність таких кроків: уявіть, що всі вони могли б працювати 24 лютого 2022 року в день вторгнення Росії в Україну. Якою б була воля України до спротиву?
- 2 СТВОРЕННЯ ЯКІСНОГО НАЦІОНАЛЬНОГО КОНТЕНТУ.** Заборонивши російські ТВ-канали та соцмережі, Україна почала підтримувати розвиток проукраїнського й україномовного продукту. Так, були вжиті заходи з підтримки української музики, кіно, телебачення, книговидавання та інших сфер.
- 3 МЕДІАОСВІТА.** Навчання населення самостійно виявляти й боротися з ворожим інформаційним впливом, у першу чергу тим, який усе ж проникає через перші два фільтри.



Розуміння важливості боротьби з ворожим інформаційним впливом вийшло з громадських і вузькоспеціалізованих ініціатив на державний рівень. Так, при Міністерстві культури та інформаційної політики України створено Центр стратегічних комунікацій та інформаційної безпеки. Питаннями боротьби з дезінформацією та ворожою пропагандою опікуються в усіх силових органах, Кабінеті Міністрів, Офісі Президента та Верховній Раді України.

● **ДЕЗІНФОРМАЦІЯ** — це свідомо подана неправдива інформація, яка поширюється, щоб завдати шкоди особі, організації або державі.

● **МІЗІНФОРМАЦІЯ** — це неправдива інформація, що поширюється без наміру завдати шкоди.

● **МАНІПУЛЯЦІЯ** — це поширення інформації (правдивої та/або неправдивої) з метою впливу на людей.

● **ФЕЙК** — це спотворена або свідомо неправдива інформація.

Центр розробив схему боротьби з дезінформацією та маніпуляцією, оскільки вони спрямовані на свідоме завдання шкоди. Схема складається з таких етапів: **ВИЯВЛЕННЯ — ЗАПОБІГАННЯ — СТРАТЕГІЧНІ КОМУНІКАЦІЇ — ОЦІНЮВАННЯ ВЖИТИХ ЗАХОДІВ**. Наступні розділи присвячені кожному етапу окремо.

ВИЯВЛЕННЯ

Для ефективної боротьби з російською дезінформацією та маніпуляцією потрібно вміти розрізняти, чи справді це частина інформаційної кампанії РФ. Це можна зробити кількома способами.

СПОСІБ 1: ВИЯВЛЕННЯ ЗА ОЗНАКАМИ

Здебільшого російська дезінформація має декілька ключових ознак, виявивши які, можна стверджувати, що це частина інформаційної війни, яку веде РФ. Список ознак складається з такого:

- цілеспрямованість: є організатор та умисел;
- елемент «неправдивості»;

- імітація, представленість як правдивого матеріалу;
- вплив на певну аудиторію через оприлюднення;
- негативні (суспільно небезпечні) наслідки;
- як правило, прив'язка до соціально значущих подій, тобто суспільно важливої інформації, що є чутливою або має символічну цінність.



ПРИКЛАД 1

ЦІЛЕСПРЯМОВАНІСТЬ. Організатор — російське пропагандистське медіа «Інформаційна агенція «Новоросія», умисел очевидний.

ЕЛЕМЕНТ «НЕПРАВДИВОСТІ». Новина абсолютно неправдива, оскільки ЗСУ не обстрілюють навіть міста, зайняті окупантами, щоб не зашкодити цивільному населенню, Миколаїв же перебуває під українським контролем, лінія фронту проходить за 30 км від нього.

ІМІТАЦІЯ. Новина представлена як правдива, згадується «джерело у місті Миколаєві», стверджується, що більшість населення міста в усіх обстрілах звинувачує ЗСУ, хоча самі ж пропагандисти в тексті новини визнають російські ракетні обстріли міста, але нібито лише «по військових об'єктах».

ВПЛИВ НА ПЕВНУ АУДИТОРІЮ. Головна цільова аудиторія — мешканці

міста Миколаєва, інші цільові аудиторії — населення підконтрольної частини України, тимчасово окупованих територій, населення РФ та незаконно створених нею псевдореспублік на території кількох країн колишнього СРСР.

НЕГАТИВНІ (СУСПІЛЬНО НЕБЕЗПЕЧНІ) НАСЛІДКИ. Вони очевидні. Новина покликана підірвати довіру в першу чергу мешканців міста Миколаєва, у другу — усього населення України до ЗСУ та влади загалом. Мета полягає в створенні негативного образу українського війська, а також приховуванні воєнних злочинів російських окупантів («переведення стрілок»).

ПРИВ'ЯЗКА ДО СУСПІЛЬНО ВАЖЛИВОЇ ІНФОРМАЦІЇ. Ракетні обстріли 500-тисячного (до повномасштабної війни) міста, які проводяться кожен день і вражають переважно цивільну інфраструктуру, — достатньо суспільно важлива інформація.

ПРИКЛАД 2

ЦІЛЕСПРЯМОВАНІСТЬ. Організатор — російський пропагандист, військовий кореспондент Олександр Сладков, умисел очевидний.

ЕЛЕМЕНТ «НЕПРАВДИВОСТІ». Новина очевидно неправдива, оскільки в ході відсічі повномасштабної військової агресії Росії ПТРК «Javelin» показали високу ефективність. Ними була знищена велика кількість одиниць техніки окупантів. Ця зброя стоїть на озброєнні армії США з 1998 року та використовується ще 19 країнами, окрім США та України. Серед них Велика Британія, Франція, Австралія, Республіка Корея, Ірландія, Чехія, Норвегія, Литва тощо. Комплекс також показав високу ефек-

тивність під час війни в Іраку, Афганістані та Сирії.

ІМІТАЦІЯ. Новина представлена як правдива. Сладков, окрім власного бачення, подає фразу «будь-який репортер, що кочує по передовій, бачив на власні очі, що солдати ЗСУ масово залишають «Javelin» на полі бою». Це робиться для підсилення «правдивості» новини.

ВПЛИВ НА ПЕВНУ АУДИТОРІЮ. Головна цільова аудиторія цієї новини — військовослужбовці ЗСУ та населення України загалом. Вона покликана деморалізувати армію та цивільних, показати «неефективність» американської зброї та перевагу над нею російської: «Були б вони такі хороші, як наш «Корнет», їх би

використовували. Був би таким легким, як РПГ-7, — понесли б з собою». Побічна цільова аудиторія — солдати російської армії та населення Росії. Мета — підбадьорити їх. Ще одна аудиторія — влада та населення західних союзників України. Їх переконують у тому, що їхня зброя неякісна, а підтримка Україні, яку вони надають, неефективна.

НЕГАТИВНІ (СУСПІЛЬНО НЕБЕЗПЕЧНІ) НАСЛІДКИ. Підрив віри ЗСУ та населення України в перемогу, ефективність озброєння, яке надають західні союз-

ники, залякування тим, що нібито російська зброя краща. Переконавання влади західних країн у тому, що їх озброєння та допомога Україні неефективні.

ПРИВ'ЯЗКА ДО СУСПІЛЬНО ВАЖЛИВОЇ ІНФОРМАЦІЇ. Джавеліни стали одним із символів спротиву ЗСУ та українського народу за допомогою країн Заходу на початковому етапі повномасштабної війни. З цим ПТРК малюють графіті та мурали, на його честь навіть називають дітей. Російські пропагандисти намагаються розбити цей символ.

СПОСІБ 2: ПОКАЗНИКИ FIRST

Показники FIRST розробила Служба урядових комунікацій Сполученого Королівства Великої Британії та Північної Ірландії (Government Communication Service).

Ці показники включають:

- **ФАБРИКАЦІЮ** (fabrication);
- **ІДЕНТИЧНІСТЬ** (identity);
- **РИТОРИКУ** (rhetoric);
- **СИМВОЛІЗМ** (symbolism);
- **ТЕХНОЛОГІЇ** (technology).

ФАБРИКАЦІЯ. Чи маніпулятивний вміст? Наприклад, підроблений документ, маніпулювання зображенням або навмисне викривлення цитати.

ГО «Детектор медіа» спростувала російський фейк про те, що нібито полк «Азов» збирається облаштувати свої позиції в житлових кварталах і що 70 % мешканців Маріуполя підтримує Росію. «Офіційний документ» на фото містить численні ознаки підробки, орфографічні та стилістичні помилки, неприродні лінгвістичні конструкції (накшталт «поребрик»), що підтверджує його несправжність.

ІДЕНТИЧНІСТЬ. Чи вказує щось на приховане або оманливе джерело або неправдиві твердження про когось іншого? Наприклад, фальшивий обліковий запис у соціальних мережах або поведінка, яка не відповідає тому, як представляється обліковий запис.

Російські пропагандисти створили фейковий телеграм-канал 14 окремої механізованої бригади імені князя Романа Великого. Окрім проукраїнських наративів, на каналі публікується і відверто неправдива інформація, така як: «більш ніж 90 % українців проти продовження мобілізації», «становище бригади критичне», «гей-активіст вступив до загону оборони Києва» тощо, тож дезінформація на цьому каналі прихована.



РИТОРИКА. Чи використовуються обтяжливий тон або фальшиві аргументи?

Фактчекерська ініціатива «Без-Брехні» розвінчала [російський міф про кількість збитих російською армією українських літаків, гелікоптерів і БПЛА](#). Річ у тому, що росіяни навели цифри, які суттєво перевищують кількість повітряної техніки, яка була на озброєнні ЗСУ до повномасштабної війни, що доводять статистичні дані міжнародних галузевих видань.

СИМВОЛІЗМ. Чи використовуються дані, проблеми чи події для досягнення непов'язаної з ними комунікаційної цілі? Наприклад, історичні приклади, вирвані з контексту, невідповідні факти для виправдання теорії змови, маніпулювання статистичними даними тощо.

Гарним прикладом цього індикатора є слова президента Путіна 23 грудня 2021 року про те, що [Україну нібито створив лідер більшовиків Владімір Ленін](#). Очевидна маніпуляція історичними прикладами, вирваними з контексту.

ТЕХНОЛОГІЇ. Чи використовуються технології як комунікаційні заходи з метою введення в оману? Наприклад, боти, діпфейки, спам тощо

[Російські хакери створили діпфейк київського міського голови Віталія Кличка та провели від його імені 20-хвилинні розмови з мерами п'яти столиць країн Європейського Союзу](#). Зловмисникам вдалося ввести в оману міських голів Варшави та Відня, проте мери Берліна, Мадрида та Будапешта ідентифікували діпфейк за деякими опосередкованими ознаками.

СПОСІБ 3: ЗІСТАВЛЕННЯ ЦІЛЬОВОЇ АУДИТОРІЇ ТА СТРАТЕГІЧНИХ НАРАТИВІВ

Інформаційна кампанія Росії зазвичай складається з кількох наративів, які активно просуваються серед певних категорій населення або всього суспільства. Уміння розпізнавати ці наративи та розуміти, на кого вони спрямовані, дозволяють усвідомити, яку загрозу і кому несуть деструктивні інформаційні дії Росії.

Шведське агентство з питань цивільного захисту розробило три способи ідентифікації стратегічних наративів на основі їх меседжу.

1 ПОЗИТИВНИЙ ЧИ КОНСТРУКТИВНИЙ: «ЦЕ ПРАВДА!»

Намагається створити цілісну розповідь про конкретну проблему, яка вписується, доповнює або розширює наявні, усталені стратегічні наративи

Прикладом є [російський дезінформаційний наратив про нібито наявність біолабораторій НАТО на території України та створення в них біологічної зброї](#). Він доповнює та розширює стратегічні наративи про те, що Україна — маріонетка країн НАТО і разом з ними загрожує національній безпеці РФ.

Продовження цього наративу — [новини про те, що нібито в крові українських військовополонених виявлені небезпечні інфекційні хвороби](#), а отже, вони піддавалися біологічним експериментам.

2

**НЕГАТИВНИЙ АБО
РУЙНІВНИЙ: «ЦЕ БРЕХНЯ!»**

Намагання запобігти появі протилежного наративу або спростувати чи підірвати вже наявний наратив.

Вдалим прикладом цього способу ідентифікації слугує наратив російської дезінформації про те, що різанина в Бучі нібито інсценована українською владою та ЗСУ. Це робиться з метою перекласти відповідальність за звірства російської окупаційної армії на Україну та відбілити свою репутацію перед міжнародною спільнотою, яку шокували кадри з Бучі.

3

**ВІДВОЛІКАЛЬНИЙ:
«ПОДИВИСЬ СЮДИ!»**

Російські пропагандисти активно відвертали увагу міжнародної спільноти від масових крадіжок українського зерна на тимчасово окупованих територіях. Для цього вони застосували контрнарратив з елементами «теорії змови» про те, нібито США та Польща забирали в України зерно, залишаючи населення голодувати. Також росіяни просували наратив про те, що українське зерно, яке експортувалося, йшло переважно до розвинених західних країн, а не до країн, що розвиваються та потерпають від нестачі продовольства. Також імовірно, що аргументовані таким чином погрози розірвати «зернову угоду» мали на меті поновлення транзиту аміаку через територію України.

Іншою частиною цього контрнарративу є маніпулятивні заяви російських високопосадовців з применшенням частки українських зернових у загальносвітовому балансі. Також вони пробували запевнити закордонну аудиторію, що війна в Україні майже не вплине на світову продовольчу безпеку.

Загалом російські стратегічні наративи виконують три базові функції. Вони або на основі ствердження створюють іншу реальність, або завдяки запереченню підривають легітимність інших наративів, або ж зменшують вагомість іншого наративу за допомогою відволікання уваги від суті.

Що ж до цільової аудиторії, на яку спрямовані стратегічні наративи, то її класифікують за масштабами й охопленням. Існують такі цільові групи:

**ШИРОКА ГРОМАДСЬКІСТЬ:
ЯКНАЙШИРША АУДИТОРІЯ**

Інформаційний вплив націлений на суспільство загалом шляхом узгодження повідомлень з широкими можливостями, спільні розповіді.

**СОЦІОДЕМОГРАФІЧНЕ
НАЦІЛЮВАННЯ: КОНКРЕТНІ ГРУПИ**

Після визначення аудиторії на основі демографічних факторів, таких як вік, дохід, освіта, етнічна приналежність тощо, повідомлення можна адаптувати для певної групи.

**ПСИХОГРАФІЧНЕ
НАЦІЛЮВАННЯ: ОСОБИ**

Аналіз і класифікація великих даних (big data) може допомогти націлити вплив на конкретну особу, поведінку якої необхідно скоригувати.

Зазвичай російська дезінформація спрямована на широку громадськість, оскільки це дозволяє досягти дестабілізації за відносно короткий час, не витрачаючи значних ресурсів на сегментування цільової аудиторії.

Дуже часто для того, щоб відповісти на запитання, чи дійсно це російська дезінформація, необхідно поєднувати перелічені вище способи. Зазвичай дезінформацію відносно легко діагностувати, однак набагато важче визначити, хто за нею стоїть. Для того, щоб переконатися в тому, що дезінформація справді російська, варто зіставити меседжі та нарративи з основними цілями Кремля, згаданими в попередніх розділах. Якщо дезінформація або маніпуляція створює позитивний образ Росії, заперечує злочинні дії її уряду або потенційно розхитує ворожість у середині українського суспільства, то в 98 % випадків — це інформаційна кампанія РФ.

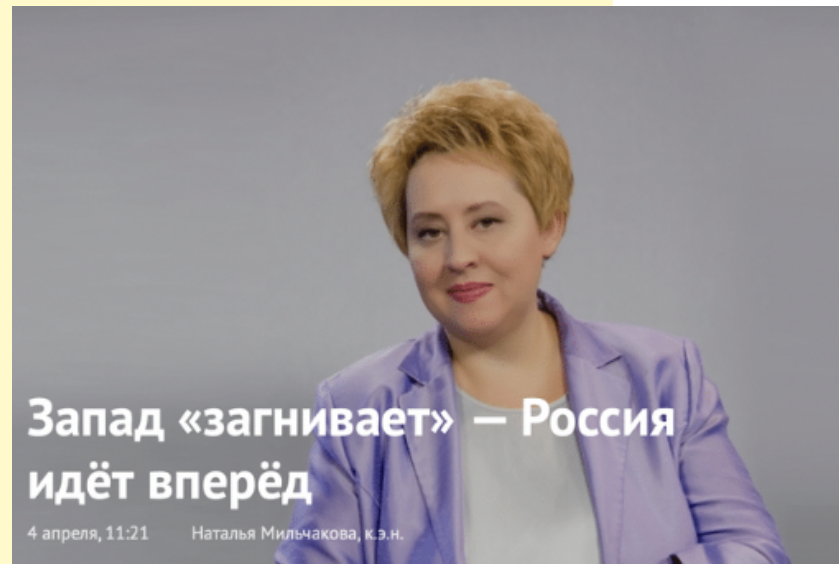
ЯК ВИЯВИТИ ФЕЙК У СОЦМЕРЕЖІ?

При визначенні того чи іншого фейку варто керуватися такими ознаками:

ДЖЕРЕЛО. На наявність фейку можуть вказувати такі особливості: відсутність джерела інформації, анонімність, ненадійність, політична заангажованість.



ЕМОЦІЇ. Якщо новина чи допис викликають сильну емоцію, це може вказувати на неправдивість інформації або її хибне висвітлення.



СПОСІБ ПОДАННЯ ІНФОРМАЦІЇ. Фейки або маніпуляції мають характерний спосіб подання: соціологічні дані без вказівки конкретних цифр; однобоке подання фактів, оцінок і коментарів, узагальнення; викривлене подання новини; неправдиві фото, відео, які використовуються на підтвердження інформації; неправильний або спотворений переклад цитати, коментаря з іноземних джерел.

Член «администрации» Запорожской области Рогов утверждает, что ООН блокировкой миссии МАГАТЭ на Запорожскую АЭС «пытается оправдать ядерный терроризм Киева», — *росСМИ*

ЕКСПЕРТНІСТЬ. Часто фейки будуються на словах певних експертів, представників структур, яких насправді не існує. Якщо в новині чи дописі згадується думка експерта без зазначення інституції, анонімний чи політично ангажований експерт, то це скоріш за все фейк або маніпуляція.

ЗАПОБІГАННЯ

Найкращий спосіб боротьби з російською дезінформацією — це недопущення її поширення на початкових етапах ІПсО. Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України пропонує низку заходів для запобігання поширенню російських наративів серед цільової аудиторії певної організації.

РОЗВИТОК МЕДІАГРАМОТНОСТІ ЦІЛЬОВОЇ АУДИТОРІЇ

Для ефективної боротьби з російською пропагандою та дезінформацією **ПОТРІБНО НЕ БОРОТИСЯ ІЗ САМИМ ЯВИЩЕМ, А ПЕРЕШКОДЖАТИ ДОСЯГНЕННЮ КОНКРЕТНИХ ЦІЛЕЙ РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ КАМПАНІЇ**. Задля цього цільову аудиторію слід робити «стійкою» до наративів і фейків, які продукує російська пропаганда.

Проведення кампаній з розвитку медіаграмотності та критичного мислення цільової аудиторії — ефективний засіб запобігання негативному впливу дезінформації. Це доводить дослідження американського аналітичного центру «RAND», у якому вказано, що після запуску програм з розвитку медіаграмотності населення користувачі соцмереж стали рідше позитивно реагувати на російські джерела незалежно від їх ідеологічної спрямованості¹⁴.

МЕДІАГРАМОТНІСТЬ — це вміння застосовувати навички критичного мислення для оцінювання повідомлень, знаків і символів, які продукуються медіа.

Таким чином, медіаграмотність допомагає визначати, аналізувати та оцінювати негативні або неправдиві меседжі, які поширюються че-

рез різні канали комунікації. Отже, що ширша аудиторія вміє застосовувати навички медіаграмотності, то важче наративам російської пропаганди проникати всередину суспільства.

ОСНОВНИЙ СПОСІБ РОЗВИТКУ МЕДІАГРАМОТНОСТІ — ПРОВЕДЕННЯ ОСВІТНІХ КАМПАНІЙ І ТРЕНІНГІВ.

В Україні такою діяльністю займається IREX (Рада міжнародних наукових досліджень та обмінів), яка реалізує проєкт «Вивчай та розрізняй: інфомедійна грамотність» (Learn to Discern). Він розпочався в Україні у 2015 році, після чого його досвід поширили на більш ніж 12 країн світу. У межах «Вивчай та розрізняй» пройшли навчання понад 400 тренерів з медіаграмотності, а всього до проєкту було залучено понад 20 000 дорослих. Серед них — учителі, освітяни закладів вищої освіти, державні службовці, журналісти, лідери громад і громадські активісти.

Діяльність проєкту в Україні спрямована, зокрема, на те, щоб навчити вчителів інтегрувати інфомедійну грамотність у свої уроки. Внаслідок цього понад 84 000 учнів на сьогодні навчаються за вдосконаленими уроками, розробленими за підтримки проєкту. Також експерти проєкту розробили загальнодоступний онлайн-курс з медіаграмотності [**«VeryVerified»**](#), доступний трьома мовами¹⁵.

i



ПОБУДОВА ДОВІРИ. Окремі категорії населення схильні мати однако-ві уподобання, інтереси та цінності, що формує приблизно однаковий пул каналів комунікації, за якими та чи інша цільова аудиторія стежить і довіряє. У зв'язку з цим для власної цільової аудиторії слід виступати легітимним джерелом, якому можна довіряти більше, ніж іншим каналам комунікації.

ОСНОВОЮ ДЛЯ ПОБУДОВИ ДОВІРИ ВИСТУПАЄ СТВОРЕННЯ ПОЗИТИВНОГО ІМІДЖУ.

Позитивний імідж включає:

- **ВІДНОСНО ЧИСЛЕННУ АУДИТОРІЮ**
- **ПІДТВЕРДЖЕНИЙ ПРОФІЛЬ У СОЦМЕРЕЖАХ**
- **БЕЗДОГАННУ РЕПУТАЦІЮ**
- **ОПЕРАТИВНІСТЬ**

ЧИСЛЕННА АУДИТОРІЯ

Користувачі схильні довіряти тим джерелам інформації, за якими стежить велика кількість людей. Для цього свої меседжі слід робити різноманітними, креативними та анімованими. Меседжі повинні бути цікавими, інклюзивними та стійкими. Цікавими меседжі робить оформлення: слід використовувати спеціалізовані відео, розповіді (stories), інтерактивні можливості. Інклюзивні меседжі передбачають поширення на якомога більшу аудиторію незалежно від віку, статі та переконань. Цього можна досягти за допомогою конкретного tone of voice* та актуальної тематики. І нарешті, стійкість визначається тим, наскільки довго та як сильно в потенційного читача зберігається меседж у свідомості.

ВЕРИФІКОВАНИЙ ОБЛІКОВИЙ ЗАПИС У СОЦМЕРЕЖАХ

Задля унеможливлення появи фейкових двійників і підвищення рівня довіри серед цільової аудиторії Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України рекомендує отримати «значок підтвердження» в соцмережах або розмістити на своєму офіційному сайті посилання на справжній профайл. Окрім цього, слід вести не односторонні комунікації, а вступати в діалог зі своєю аудиторією задля створення відчуття спілкування та надання аудиторії можливості бути почутою.

БЕЗДОГАННА РЕПУТАЦІЯ

Бездоганна репутація передбачає дотримання неформального етичного кодексу — непоширення дезінформації, закликів до насильства та мови ненависті. Ці та інші принципи, яких слід дотримуватися при реалізації комунікаційної кампанії, викладені в документі під назвою [«Кодекс етики українського журналіста»](#). Особливо важливими компонентами якісних комунікацій виступають також прозорість, правдивість, відкритість, справедливості і точність.

Публікація фейків, які були викриті, підриває довіру цільової аудиторії та негативно впливає на подальшу репутацію та діяльність організації.

*Tone of voice — манера, у якій певний канал комунікації доносить інформацію до власної аудиторії.

¹⁴ Todd C. Helmus, James V. Marrone, Marek N. Posard, Danielle Schlang. Russian Propaganda Hits Its Mark. Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions [\(Електронний ресурс\)](#)



¹⁵ Katya Vogt. What we learned about building resilience to manipulative information from Learn to Discern [\(Електронний ресурс\)](#)



Навіть позитивні для України новини, які є фейками (наприклад, смерть гауляйтера окупованої Херсонської області Володимира Сальда, узяття ЗСУ села Киселівки під Херсоном або референдум у Белгородській області РФ), шкодять і загрожують репутації наших державних органів і медіа.

Прикладом може слугувати скандал, пов'язаний з діяльністю колишньої Уповноваженої з прав людини Верховної Ради України Людмили Денісової. Відповідно до незалежного журналістського розслідування, Людмила Денісова поширювала фейки про зґвалтування російськими окупантами українських дітей і жінок. Як наслідок, у населення підірвана довіра до інституту Уповноваженого

з прав людини, а російська пропаганда отримала новий інструмент впливу для відбілювання своєї репутації¹⁶.

ОПЕРАТИВНІСТЬ

У реаліях нинішнього інформаційного середовища швидкість оприлюднення інформації надзвичайно важлива. Оперативне висвітлення тієї чи іншої події або ж належна і своєчасна реакція залучає широку аудиторію та тим самим збільшує її довіру. Боротьба за довіру між різними каналами та джерелами інформації — це переважно «гра з нульовою сумою», тобто підвищення довіри до одного джерела зменшує довіру до іншого. Саме тому вкрай необхідно виборювати довіру в населення, щоб зменшувати можливі масштаби впливу російської пропаганди.

СТРАТЕГІЧНІ КОМУНІКАЦІЇ

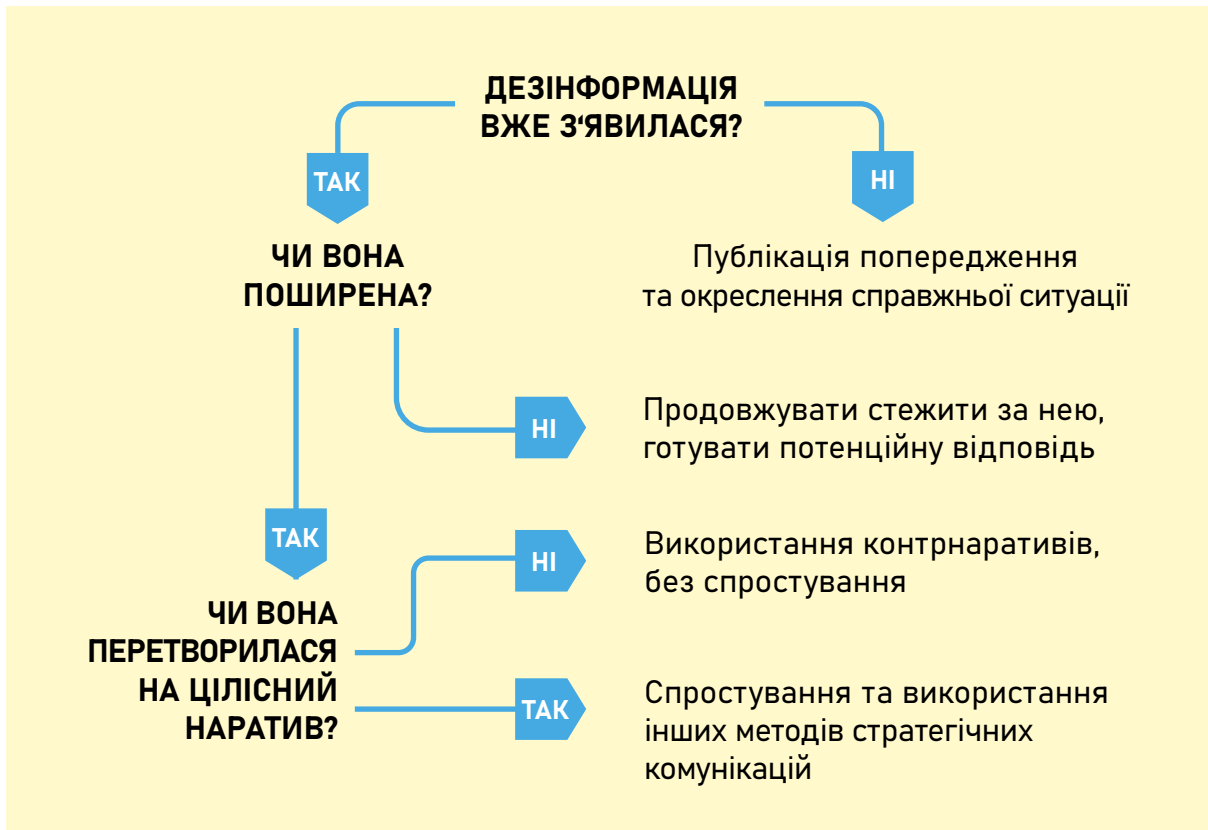
Після виявлення російської дезінформації слід розробити шляхи боротьби з нею. Одним з ключових інструментів запобігання поширенню дезінформації є регулярне використання основ стратегічних комунікацій — методів, принципів і каналів поширення.

Утім, спочатку потрібно визначити доцільність таких дій. Не кожен фейк чи дезінформація потребують реагування. Якщо дезінформація не становить жодної загрози діяльності організації та її аудиторії, то боротьба з фейком може лише погіршити ситуацію, спричинивши ефект зворотного результату. Цей феномен полягає в тому, що постійне повторення фейку в контексті його спростування може закріпити його в головах аудиторії як правдиву інформацію. Принцип такий: повторення інформації робить її знайомою; людський мозок схильний більше довіряти знайомій інформації, яка йому вже траплялася раніше.

Саме тому слід ретельно оцінювати фейки та дезінформацію, з якими треба боротися, ґрунтуючись на масштабі впливу на аудиторію.

Центр стратегічних комунікацій пропонує схему для визначення необхідності боротьби з дезінформацією:

- ▶ якщо дезінформація ще не з'явилася — попередити аудиторію про можливу дезінформацію та окреслити справжню ситуацію;
- ▶ якщо дезінформація вже з'явилася, однак не поширилася — продовжувати стежити за нею, готувати потенційну відповідь;



► якщо дезінформація вже з'явилася й почала масово поширюватися, однак це окремі меседжі, що не перетворилися на наратив або підпадають під один з наявних загальних наративів, — використати контрнарративи, без спростування;

► якщо дезінформація вже з'явилася й почала масово поширюватися, а окремі меседжі перетворилися на наратив — спростувати та використати інші методи стратегічних комунікацій.

НАРАТИВ — це загальне спрощене висвітлення окремої проблеми, що формує певну точку зору в потенційного читача.

МЕСЕДЖ — це складова частина наративу, яка стосується конкретного явища, події чи ситуації.

Дослідницька служба Європейського парламенту визначає¹⁶ дезінформацію як ключовий компонент гібридних за-

гроз, а стратегічні комунікації — як основний та ефективний засіб боротьби з нею. Загалом існує безліч визначень поняття «стратегічні комунікації». У Воєнній доктрині України стратегічні комунікації розуміються як **«СКООРДИНОВАНЕ І НАЛЕЖНЕ ВИКОРИСТАННЯ КОМУНІКАТИВНИХ МОЖЛИВОСТЕЙ ДЕРЖАВИ — ПУБЛІЧНОЇ ДИПЛОМАТІЇ, ЗВ'ЯЗКІВ ІЗ ГРОМАДСЬКІСТЮ, ВІЙСЬКОВИХ ЗВ'ЯЗКІВ, ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ, ЗАХОДІВ, СПРЯМОВАНИХ НА ПРОСУВАННЯ ЦІЛЕЙ ДЕРЖАВИ»**.

¹⁶ Соня Лукашова. Від facebook до допитів. Чому омбудсмен Денісова втратила посаду [\(Електронний ресурс\)](#)



¹⁷ Panel for the Future of Science and Technology. Strategic communications as a key factor in countering hybrid threats [\(Електронний ресурс\)](#)



ОСНОВНІ ХАРАКТЕРИСТИКИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ:

■ втілюються відповідно до складеного та систематичного плану, а не лише у відповідь на певну подію;

■ передбачають дії на стратегічному, операційному та тактичному рівнях;

■ створені в конкурентному середовищі;

■ потребують високого рівня скоординованості та синхронізації між основними стейкхолдерами / зацікавленими сторонами;

■ потребують визначення цільової аудиторії;

■ потребують визначення найбільш релевантних каналів комунікації;

■ потребують встановлення мети інформування, впливу та зміни поведінки цільової аудиторії;

■ відповідають загальним цілям організації;

■ мають коротко-, середньо- та довгострокові цілі.

ОСНОВНІ ПРИНЦИПИ:

ЗОСЕРЕДЖЕННЯ НА ЛІДЕРСТВІ:

лідери організації повинні долучатися до затвердження та контролювати реалізацію стратегічних комунікацій

ПРАВДИВІСТЬ:

такі цінності, як точність, правдивість, надійність і послідовність, повинні враховуватися при реалізації стратегічних комунікацій

РОЗУМІННЯ: стратегічні комунікації вимагають докладати зусиль, щоб знати та розуміти культуру, бачення, ідентичність, історію, ставлення, поведінку та соціальні цінності цільової аудиторії

ДІАЛОГ:

потрібно враховувати обмін ідеями між усіма залученими учасниками

ГНУЧКІСТЬ:

цілі та засоби повинні швидко змінюватися залежно від зовнішніх умов

ПРОДОВЖУВАНІСТЬ: стратегічні комунікації — це тривалий процес досліджень, збору інформації, аналізу, планування, впровадження, оцінювання та адаптації

ВСЕПРОНИКНІСТЬ:

основні меседжі повинні доходити до якомога більшої кількості учасників цільової аудиторії

ОРІЄНТОВАНІСТЬ НА РЕЗУЛЬТАТ:

стратегічні комунікації повинні мати чіткі цілі та засоби їх досягнення

КЛЮЧОВІ КОМПОНЕНТИ:

ОЧІКУВАНИЙ РЕЗУЛЬТАТ, АУДИТОРІЯ, МЕСЕДЖ, МЕТОДИ Й КАНАЛИ КОМУНІКАЦІЙ ТА ОЦІНЮВАННЯ ВПЛИВУ.



У боротьбі з російською дезінформацією очікуваним результатом стратегічних комунікацій зазвичай виступає **ЗМЕНШЕННЯ НЕГАТИВНОГО ВПЛИВУ РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ**.

Російська дезінформаційна діяльність здебільшого **СПРЯМОВАНА НА ЯКОМОГА ШИРШУ ЦІЛЬОВУ АУДИТОРІЮ** (див. пункт «Запобігання»). Утім, існують і кампанії, націлені на певну демографічну групу. Відповідно боротьба з російською дезінформацією повинна спрямовуватися на таку ж за масштабом аудиторію.

Канали стратегічних комунікацій бувають трьох типів — **СПІЛКУВАННЯ ВІЧ-НА-ВІЧ, МЕДІА ТА СОЦІАЛЬНІ МЕРЕЖІ**.

КАНАЛ	ВИД	СПРЯМУВАННЯ	ПЕРЕВАГИ	НЕДОЛІКИ
СПІЛКУВАННЯ ВІЧ-НА-ВІЧ	■ брифінг ■ зустріч з громадою ■ виступ на заході	■ побудова довіри ■ інформування про нагальні питання та події ■ особливо важливі оголошення	■ покращення репутації організації ■ налагодження діалогу ■ аудиторія відчуває себе почутою та важливою	■ охоплення вузької аудиторії ■ неможливість організації через несприятливі умови
МЕДІА	■ пресреліз ■ інтерв'ю ■ коментар ■ прес-конференція	■ роз'яснення ситуації ■ поліпшення іміджу ■ просування наративу	■ підвищення довіри за допомогою джерела ■ реалізація проміжних цілей комунікаційної стратегії ■ оптимізація ресурсів	■ ризик неотримання меседжу цільовою аудиторією

КАНАЛ	ВИД	СПРЯМУВАННЯ	ПЕРЕВАГИ	НЕДОЛІКИ
СОЦІАЛЬНІ МЕРЕЖІ	■ дописи ■ розповіді ■ прямі трансляції ■ відео- та аудіоматеріали	■ інформування про нагальні питання та події ■ особливо важливі оголошення ■ роз'яснення ситуації ■ реакція на основні події просування меседжів і наративу ■ реалізація стратегічних цілей комунікаційної кампанії	■ широке охоплення аудиторії ■ можливість зворотного зв'язку ■ інформування про нагальні питання та події ■ можливість відстеження впливу комунікаційної стратегії	■ ризик атаки ботів і тролів ■ імовірність зламу профілю ■ можливість отримання санкцій від соцмереж за «мову ворожнечі» або інші формальні порушення

Методи стратегічних комунікацій поділяють на **ПРОАКТИВНІ** та **РЕАКТИВНІ**.

ПРОАКТИВНІ МЕТОДИ спрямовані на забезпечення правдивої та своєчасної інформації для цільової аудиторії перед виникненням інформаційної маніпуляції, а також на побудову стійкості тієї ж аудиторії до неправдивих наративів.

До них належать:

- **ВИЗНАЧЕННЯ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА;**
- **КОМУНІКАЦІЙНІ СТРАТЕГІЇ;**
- **ПІДВИЩЕННЯ ОБІЗНАНОСТІ;**
- **ПРЕБАНКІНГ;**
- **НАЛАГОДЖЕННЯ ПАРТНЕРСЬКОЇ МЕРЕЖІ;**
- **ВИБУДОВА СТІЙКОСТІ ЦІЛЬОВОЇ АУДИТОРІЇ.**

ВИЗНАЧЕННЯ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Інформаційне середовище — це теоретична концепція, яка описує взаємодію тих, хто ретранслює інформацію, і тих, хто її отримує; бачення аудиторією світу навколо себе на основі її переконань, цінностей та інтересів. Інформаційне середовище складається з трьох взаємопов'язаних вимірів: **КОГНІТИВНОГО** (коли люди думають, розуміють і вирішують), **ФІЗИЧНОГО** (окремі особистості, організації тощо) та **ІНФОРМАЦІЙНОГО** (факти, знання та інформаційні дані)¹⁸.

Аналіз інформаційного середовища потрібен для того, щоб усвідомлю-



вати вразливості своєї цільової аудиторії і відповідно до цього розуміння вибудовувати комунікаційну стратегію, встановлювати цілі та проводити заходи.

Під вразливостями слід розуміти нездатність протистояти деструктивному інформаційному впливу, зумовлену соціальними, психологічними, культурними та комунікаційними вадами й проблемами. Вразливості породжують слабкість державних, економічних, соціальних і громадських інститутів на всіх рівнях, яка потенційно може перешкоджати ефективному існуванню державного та суспільного життя.

В Україні вразливості часто пов'язані з погіршенням соціального забезпечення, відсутністю реформ, громадянськими заворушеннями, недовірою до уряду, мовним питанням і війною Росії проти нашої держави¹⁹.

КОМУНІКАЦІЙНА СТРАТЕГІЯ

Призначена для вироблення чіткого плану донесення конкретних меседжів до цільової аудиторії заради реалізації певних організаційних і комунікаційних цілей.

Вироблення комунікаційної стратегії стає можливим після аналізу інформаційного середовища, описаного раніше. Таким чином, при створенні та реалізації комунікаційної стратегії слід враховувати такі сім компонентів:

1

ЦІЛЬОВА АУДИТОРІЯ: її потреби, інтереси та цінності;

2

ОРГАНІЗАЦІЙНІ ЦІЛІ: чого хоче досягти організація;

3

КОМУНІКАЦІЙНІ ЦІЛІ: як досягнути цілей організації за допомогою комунікації з цільовою аудиторією;

4

МЕСЕДЖІ: що організація хоче донести до цільової аудиторії;

5

КАНАЛИ КОМУНІКАЦІЇ: яким чином найкраще доносити інформацію до цільової аудиторії;

6

ЧАСОВІ РАМКИ: коли меседжі повинні досягти цільової аудиторії;

7

ОЦІНЮВАННЯ ВПЛИВУ: чи досягла комунікаційна стратегія бажаного результату.

Часто боротьба з російською дезінформацією або запобігання їй є інтеграційною складовою комунікаційних стратегій, які мають на меті більш широкі цілі.

ПІДВИЩЕННЯ ОБІЗНАНОСТІ

Спрямоване на створення стійкого уявлення про явище, подію чи ситуацію в цільовій аудиторії. Підвищення обізнаності може бути однією з цілей комунікаційної стратегії. Її можна досягти за допомогою навчальних програм, публічних лекцій і виступів, поширення просвітницького контенту, заохочення до самоосвіти, різних форм обміну професійними знаннями й досвідом.

¹⁸ U.S. Joint Chiefs of Staff, Joint Publication 3-13: Information Operations, incorporating change 1 (Washington D. C., 2014), 1-2.

¹⁹ Internews Ukraine. Taming the Hydra. How to Resist Kremlin's Information Aggression ([Електронний ресурс](#))



У контексті боротьби з російською дезінформацією підвищення обізнаності може бути спрямоване на поширення знань серед населення про історію державності України, досягнення українського народу для викорінення синдрому меншовартості, імплементацію реформ, євроатлантичного курсу, діяльність влади під час війни.

Хорошим прикладом таких комунікацій можуть слугувати сторінки Віцепрем'єр-міністерки з питань європейської інтеграції Ольги Стефанішиної. На них вона звітує про конкретні кроки щодо поглиблення співробітництва України з країнами ЄС, роботу над узгодженням українського законодавства з європейськими стандартами тощо.

Історичними питаннями вже давно та успішно опікується Український інститут національної пам'яті. Ця структура популяризує академічні знання з історії, протидіє російсько-радянському історичному наративу, змогла суттєво змінити ставлення українців до свого минулого, публічно засудити численні злочини комуністичного та нацистського режимів на території України.

ПРЕБАНКІНГ (PREBUNKING) — попередження аудиторії про можливу появу дезінформаційного меседжу або наративу. Це один з найефективніших інструментів стратегічних комунікацій у боротьбі з російською дезінформацією, оскільки нівелює вплив інформаційної кампанії ще до її початку чи масового поширення. Передбачити виникнення російської дезінформації можна за допомогою оцінювання ризиків і медіамоніторингу.

Оцінювання ризиків — визначення, які з вразливостей цільової аудиторії найімовірніше будуть експлуатувати агенти ворожої інформаційної кампанії.

Окрім цього, пребанкінгу сприяє розвідувальна інформація спецслужб. Утім, вона доступна лише на вищих щаблях державних структур і часто не підлягає розголошенню.

Головне управління розвідки Міністерства оборони України систематично публікує на своїх сторінках попередження про нові хвилі російських ІПсО, маніпуляцій, фейків і дезінформації.

Так, у серпні 2022 року українські розвідники оприлюднили інформацію про те, що російські пропагандисти готують запуск підробного сайту нібито Фонду Володимира

Зеленського для дискредитації Президента України.

Генеральний штаб ЗСУ попереджував про ймовірні провокації росіян під час «Армійських міжнародних ігор — 2022», що відбулися в Білорусі у серпні 2022 року. Таким чином, можливо, вдалося запобігти сценарію диверсій з жертвами серед військовослужбовців іноземних країн.



НАЛАГОДЖЕННЯ ПАРТНЕРСЬКОЇ МЕРЕЖІ

Виступає важливою складовою не лише комунікаційної діяльності певної організації, а й усієї державної і суспільної комунікаційної структури.

Спільна позиція всіх відомств та установ країни — необхідна передумова побудови стійкості суспільства до російської дезінформації. Державні органи разом з громадськими організаціями мають дотримуватися одного визначеного комунікаційного курсу, просувати одні й ті ж меседжі та наративи і вибудовувати спільний бренд, який важко було б зруйнувати російській пропаганді. Іншими словами, комунікаційний процес в Україні повинен здійснюватися відповідно до політики «одного голосу».

Окрім цього, партнерство з іншими державними інституціями, медіа та громадськими організаціями розширить коло охопленої аудиторії. Завдяки поширенню у соціальних мережах, публікації новин у виданнях боротися з російською дезінформацією легше, оскільки велика кількість населення дізнається про ті чи інші дезінформаційні наративи та їх хибність.

Важливе місце в інформаційному просторі сьогодення займають інфлюенсери — блогери, громадські активісти та культурні діячі. Їх залучення до процесу комунікації дасть поштовх якісному та швидкому поширенню основних меседжів та наративів, які б нівелювали вплив російської дезінформації.

Прикладом неузгоджених і нескоординованих комунікацій може слугувати випадок розпорядження Генерального штабу ЗСУ про заборону чоловікам покидати межі областей, де вони проживають, без дозволу військкоматів. Генштаб не узгодив це рішення з вищим політичним керівництвом держави, що призвело до його скасування Президентом України та хвилі критики не лише серед суспільства, а й депутатів Верховної Ради України, які навіть зареєстрували проєкт постанови про скасування цього розпорядження.

У самому Генштабі та Міністерстві оборони України також не було єдиної позиції щодо тлумачення нововведення. Так, Головнокомандувач ЗСУ Валерій Залужний і речник Міністерства оборони України Олександр Мотузник підтвердили обмеження на пересування чоловіків усередині України, тоді як [юридична радниця Залужного Євгенія Рябека заявила, що військовозобов'язані чоловіки можуть пересуватися Україною без будь-яких дозволів.](#)

Безумовно, подібні ситуації сильно шкодять іміджу держави та ЗСУ. Ця історія сприяла російській пропаганді, яка відразу ж розіграла карту нібито «конфлікту між Зеленським і Залужним», порушення прав людини в Україні тощо.

ВИБУДОВА СТІЙКОСТІ. Стійкість цільової аудиторії означає здатність населення не піддаватися деструктивному інформаційному впливу. Детальніше про це йдеться в пункті «Запобігання».

РЕАКТИВНІ МЕТОДИ стратегічних комунікацій використовуються після виникнення дезінформаційних меседжів і наративів та спрямовуються на їх заперечення й нівелювання.

До них належать:

- **«НАЗВАТИ Й ЗАСУДИТИ» (NAMING-AND-SHAMING);**
- **СПРОСТУВАННЯ;**
- **КОНТРНАРАТИВ;**
- **КРИЗОВІ КОМУНІКАЦІЇ.**

«НАЗВАТИ Й ЗАСУДИТИ» —

це інструмент стратегічних комунікацій, який передбачає публічне розкриття та звинувачення в розповсюдженні дезінформації особи чи організації. У контексті боротьби з російською дезінформацією розкриття осіб, медіа чи акаунтів у соціальних мережах, які розповсюджують російські дезінформаційні наративи, підриває довіру аудиторії до цих каналів комунікації та надалі зводить нанівець негативний вплив російської пропаганди.

Так, Служба безпеки України України періодично [публікує та оновлює списки телеграм-каналів, що просувають ворожу пропаганду](#), адже їх кількість невинно зростає.

СПРОСТУВАННЯ

Спростування дезінформації — один з найважливіших і найефективніших засобів стратегічних комунікацій у боротьбі з російською дезінформацією.

СПРОСТУВАННЯ — це викриття неправдивої інформації та наведення правдивих контраргументів. Загальна мета спростування — зменшення негативного впливу дезінформації.

Часто **СПРОСТУВАННЯ** супроводжується **ФАКТЧЕКІНГОМ**, однак ці два інструменти дещо відрізняються²⁰. Якщо **ФАКТЧЕКІНГ** доволі широке поняття, то спростування фокусується на певній проблемі.

СПРОСТУВАННЯ починається з визначення, чию інформацію потрібно спростовувати на основі оцінювання намірів і поведінки.

Окрім цього, **СПРОСТУВАННЯ** — це стратегічний інструмент. Якщо **ФАКТЧЕКІНГ** зосереджується на пошуку правди незалежно від природи дезінформації, то спростування застосовується лише до тієї дезінформації, яка потенційно може зашкодити інтересам і цілям певної організації.

ФАКТЧЕКІНГ — довгий і ресурсозатратний процес. На відміну від спростування його часто віддають на аутсорс. В Україні існує кілька фактчекінгових організацій, до яких можна звернутися по допомогу або встановити партнерство заради спільної боротьби з російською дезінформацією. Їх перелік наведено в Додатках.

СПРОСТУВАННЯ може робити сама організація. Утім, потрібно дотримуватися певного алгоритму, щоб уникнути **ПІДТВЕРДЖУВАЛЬНОГО УПЕРЕДЖЕННЯ** або **ЕФЕКТУ ЗВОРОТНОГО ВПЛИВУ**.

²⁰ James Pamment, Anneli Kimber Lindwall. Fact-checking and debunking. A best practice guide to dealing with disinformation. NATO Strategic Communications Centre of Excellence.



ЗАГАЛЬНОПРИЙНЯТА СТРУКТУРА СПРОСТУВАННЯ ДЕЗІНФОРМАЦІЇ:

1 ■ ФАКТ

Текст повинен починатися з чіткого, простого та зрозумілого факту, щоб встановити стійке уявлення про проблему в потенційного споживача.

2 ■ ПОПЕРЕДЖЕННЯ ПРО МІФ

Потрібно розповісти, яку дезінформацію розповсюджують. Описати неправдиву інформацію лише раз і доволі коротко.

3 ■ ОБҐРУНТУВАННЯ ХИБНОСТІ

Навести сильні аргументи, які б довели неправдивість та маніпулятивність розповсюджуваної дезінформації.

4 ■ ФАКТ Повторити факт у вигляді підсумку.

ПРИКЛАД

■ **ФАКТ.** Україна НЕ виробляє біологічної зброї.

■ **ПОПЕРЕДЖЕННЯ ПРО МІФ.** Однак російська пропагандистська машина стверджує протилежне.

Ще до повномасштабного вторгнення Росії в Україну російські ЗМІ оприлюднювали фейки, нібито в Україні існують створені Заходом лабораторії, які виробляють біологічну зброю. Після 24 лютого 2022 року таку риторику почали застосовувати на офіційному рівні. Так, наприклад, Дмитрій Медведєв заявив, що Росія має докази того, що метою створення біолабораторій США в Україні була розробка біологічної зброї. Понад те, 11 березня РФ скликала засідання Ради Безпеки ООН, де заявила, що Україна спільно із США розробляє біологіч-

ну зброю. Згодом з цього приводу Росія скликала ще два засідання — 18 березня та 13 травня.

■ ОБҐРУНТУВАННЯ ХИБНОСТІ.

Утім, на всіх трьох засіданнях Ради Безпеки ООН Ідзумі Накаміцу, Верховний представник ООН з питань роззброєння, зазначав, що ООН не знає про існування будь-якої програми біологічної зброї в Україні. Також Державний департамент США заперечив факт існування лабораторій в Україні, які б виготовляли біологічну зброю.

Насправді США та Україна співпрацюють у сфері біологічної безпеки, а не у сфері розробки біологічної зброї.

Співпраця здійснюється в межах Програми зі зменшення біологічної загрози (Biological Threat Reduction Program, BTRP), яка є частиною Програми спільного зменшення загроз (Cooperative Threat Reduction,

²¹ Lewandowsky S., Cook J., Ecker U. K. H., Albarracín D., Amazeen M. A., Kendeou P., Lombardi D., Newman E. J., Pennycook G., Porter E., Rand D. G., Rapp D. N., Reifler J., Roozenbeek J., Schmid P., Seifert C. M., Sinatra G. M., Swire-Thompson B., van der Linden S., Vraga E. K., Wood T. J., Zaragoza M. S. The Debunking Handbook 2020 ([Електронний ресурс](#))



CTR) Міністерства оборони США. Ця програма реалізується спільно з урядом України з 2005 року. Мета — підтримка мирних і безпечних досліджень, діагностики та зменшення біологічних загроз, які становлять патогени.

Під час виконання Програми зі зменшення біологічної загрози було [модернізовано](#) багато лабораторій Міністерства охорони здоров'я України та Державної служби України з питань безпечності харчових продуктів і захисту споживачів. У 2019 році побудовано дві лабораторії (у Києві та Одесі).

До того ж Україна є державою-учасницею Конвенції про біоло-

гічну зброю 1972 року. Конвенція [забороняє](#) розробляти, виробляти та накопичувати запаси бактеріологічної зброї.

■ **ФАКТ.** Отже, Росія бреше про біологічну зброю в Україні заради виправдання неспровокованого повномасштабного вторгнення на територію Української держави. Доволі іронічно, що звинувачення у виробництві біологічної зброї висуває країна, яка застосовувала заборонену хімічну та біологічну зброю проти цивільних громадян в Алеппо (Сирія) та усувала в такий спосіб невідгук для кремлівського режиму людей (Олександра Литвиненка, Сергія Скрипаля тощо).

КОНТРНАРАТИВ — ЦЕ ПРОСУВАННЯ ВЛАСНОГО НАРАТИВУ НА ПРОТИВАГУ МАНІПУЛЯЦІЯМ І ДЕЗІНФОРМАЦІЇ КОНТРАГЕНТА. Часто контрнарратив використовується для висвітлення власної точки зору щодо надзвичайно чутливого та неоднозначного питання.

Контрнарратив потребує **ЗЛАГОДЖЕНОГО ПРОЦЕСУ КОМУНІКАЦІЇ ВСІХ СТЕЙКХОЛДЕРІВ, ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ СПРОСТУВАННЯ ТА ПОСТІЙНОГО ОБҐРУНТУВАННЯ СВОЇЇ ПОЗИЦІЇ ФАКТАМИ.**

У контексті боротьби з російською дезінформацією контрнарратив займає важливе місце в побудові позитивного іміджу України як серед населення Української держави, так і міжнародної спільноти.

Яскравий приклад **СТРАТЕГІЧНОГО КОНТРНАРАТИВУ** України — заперечення російського пропаган-

дистського наративу про те, що ворожі війська проводять на нашій території нібито «спеціальну військову операцію» та завдають ударів лише по військових об'єктах. Президент України та інші представники української влади систематично розповідають світові про навмисні воєнні злочини російської армії, спрямовані винятково проти мирного населення, надають переконливі факти та докази.

Журналісти [«Hromadske»](#) та New York Times надали переконливі фотодокази звірств окупаційної російської армії проти цивільного населення в Бучі. Подібні розправи над мирним і беззбройним населенням не можуть бути виправдані жодною військовою необхідністю. [Президент Володимир Зеленський активно комунікував цю жахливу історію, зокрема і перед міжнародною спільнотою.](#)

27 червня 2022 року [російські окупанти завдали ракетний удар по торго-](#)

[вельному центру «Амстор» у Кременчуку Полтавської області.](#) На момент удару там перебувало близько 1 000 людей. Унаслідок цілеспрямованої атаки на цивільне населення загинула 21 людина, 101 особа була поранена, ще одна — зникла безвісти. Аналітики [«Bellingcat»](#) переконливо спростували всі можливі брехливі версії російських пропагандистів щодо військової цілі цього удару. Слід зауважити, що ці версії були, як завжди, дуже різними та суперечили одна одній, що є характерною ознакою окупантів-дезінформаторів. [Президент України показав відео ракетного удару у своєму зверненні.](#)

14 липня 2022 року [росіяни завдали ракетного удару по центру Вінниці,](#) внаслідок якого загинули 26 осіб, були поранені 202 людини, ще восьмеро зникли безвісти. Згідно із заявою вінницького міського голови Сергія Моргунова, [у радіусі двох кілометрів від місця удару немає жодного військового об'єкта української армії.](#) [Президент України Володимир Зеленський опублікував відео](#) з наслідками ракетного удару й назвав Росію країною-терористом.

Ще одним **КОНТРНАРАТИВОМ** є **ДЕКОМУНІЗАЦІЯ**. Російська пропаганда вже близько двох десятиліть активно використовує радянське минуле та комуністичні символи для просування своїх цілей, вони стали її невіддільною частиною. Українська влада від 2014 року провадить системну політику декомунізації, здійснюється активна робота з раніше засекреченими, а нині відкритими архівами спецслужб, ґрунтовні історичні дослідження. Завдяки зусиллям державних структур, науковців, активістів викрито чимало страшних і кривавих злочинів ко-



муністичного режиму. Це розбиває російський пропагандистський наратив про те, як у СРСР «добре і безпечно жилося», про «дружбу братніх народів» тощо.

КРИЗОВІ КОМУНІКАЦІЇ ОЗНАЧАЮТЬ ЗДІЙСНЕННЯ ПРОЦЕСУ КОМУНІКАЦІЇ З ЦІЛЬОВОЮ АУДИТОРІЄЮ В УМОВАХ КРИЗИ.

Під кризою можна розуміти широкий перелік явищ і подій — від стихійних лих до корупційного скандалу, від атак на критичну інфраструктуру до відставки очільника відомства.

Критичні ситуації створюють сприятливі умови для швидкого поширення дезінформації. Саме тому дотримання основних принципів і використання головних інструментів кризових комунікацій надзвичайно важливе для будь-якої організації.

ПРОЦЕС КРИЗОВИХ КОМУНІКАЦІЙ СКЛАДАЄТЬСЯ З ДЕКІЛЬКОХ ЧАСТИН.

1 ■ ВИЗНАЧЕННЯ ЗАГРОЗ

На цій стадії завдяки аналізу інформаційного середовища та визначенню вразливостей слід передбачити можливі кризові сценарії та розподілити їх від найбільш до найменш ймовірного.

2 ■ ПІДГОТОВКА

Стадія підготовки передбачає завчасне вироблення стратегії відповіді на кризову ситуацію — визначення основних меседжів, розподілення обов'язків, встановлення основних каналів комунікації.

3 ■ ВІДПОВІДЬ

Реакція на кризову ситуацію повинна бути швидкою та спільною в усіх стейкхолдерів. Окрім цього, відповідь повинна викликати довіру в цільовій аудиторії та встановити зв'язок з нею.

4 ■ ОЦІНЮВАННЯ. Після того, як криза минула і стратегія була застосована, слід виміряти ефективність використаного плану кризових комунікацій. На основі аналізу внести корективи до майбутніх кризових комунікаційних планів.

У 2020 році в межах діяльності проєкту міжнародної технічної допомоги «Партнерство для розвитку міст» був підготовлений практичний посібник [«Довіра громади: кризові комунікації органів місцевого самоврядування»](#), який містить детальний опис розробки кризових комунікацій і їх застосування.

У контексті боротьби з російською дезінформацією під час війни кризові ситуації трапляються дуже часто і зазвичай вони пов'язані з атаками РФ як на військові, так і цивільні об'єкти в Україні. Застосування кризових комунікацій в умовах воєнного часу допоможе уникнути поширення паніки серед населення і зневіри в перемозі України.

ОЦІНЮВАННЯ ВЖИТИХ ЗАХОДІВ

Оцінювання стратегічних комунікаційних кампаній — останній і вкрай важливий етап циклу з протидії дезінформації. Воно дозволяє виявити та проаналізувати якість проведеної комунікаційної кампанії, зрозуміти для себе її вплив на цільову аудиторію, неточності та помилки.

АНАЛІЗ результатів оцінювання дозволяє краще ознайомитися з потребами та реакціями аудиторії на певні комунікаційні меседжі та заходи. Успішні приклади можна використовувати й

надалі, адаптувати до інших ситуацій. Ті ж комунікаційні стратегії, що продемонстрували свою неефективність, у майбутньому можна замінити на інші, відкоригувати та посилити.



Це підвищить імовірність того, що цільова аудиторія суттєво зацікавиться контентом, тим самим зменшуючи її вразливість до дезінформації. Після адаптації стратегії та запуску нової комунікаційної кампанії важливо знову **ВІДСТЕЖУВАТИ ЕФЕКТИВНІСТЬ**.

Базові показники є важливою частиною вимірювання на початку комунікаційної кампанії. Вимірювання базових показників дозволяє чітко зрозуміти, чи досягли бажаного результату застосовані інструменти та канали комунікації. Варто зауважити, що оцінювання впливу вжитих заходів повинно бути повторюваним процесом.

ЯК ВИМІРЯТИ ЕФЕКТИВНІСТЬ СТРАТЕГІЧНОЇ КОМУНІКАЦІЇ?

У контексті боротьби з російською дезінформацією оцінювання проведених заходів повинно ґрунтуватися на цілях стратегічних комунікацій. Можемо виділити шість основних цілей, починаючи з тактичних і закінчуючи стратегічними:

1 ЗАЛУЧЕННЯ ВРАЗЛИВОЇ АУДИТОРІЇ. Важливо «утримувати» аудиторію, яка найбільш схильна піддаватися російській пропаганді, у своєму інформаційному полі, щоб унеможливити вплив на неї російської дезінформації. Прогрес досягнення цієї цілі можна визначити за базовими метриками: демографічні особливості (вік, стать, географічне розташування) підписників у соцмережах, глядачів телеканалу, читачів видання та їх кількість.

2 ПОБУДОВА ДОВІРИ. Залучена аудиторія повинна сприймати організацію як джерело правдивої інформації. Результат цієї цілі можна визначити за динамікою залучення аудиторії, кількістю посилань на ін-

формацію від організації, кількістю згадок у медіа та фігуруванням в інформаційному просторі.

3 ПІДВИЩЕННЯ ОБІЗНАНОСТІ. Дезінформація виникає там, де бракує об'єктивних знань. Якщо аудиторія достатньо обізнана про певну проблему, імовірність виникнення маніпуляцій або дезінформації різко знижується. Досягнення такої цілі залежить від охоплення аудиторії, її реакції та засвоєння інформації.

4 ВИБУДОВА СТІЙКОСТІ. Щоб уникнути подальшого розповсюдження дезінформаційного контенту серед цільової аудиторії, потрібно навчити її відрізняти правду від неправди. Раніше ми розповідали, як цього досягти. Вимірювання прогресу досягнення стійкості цільової аудиторії можна проводити за допомогою опитувань та анкетувань.

5 ЗМІНА ПЕРЕКОНАНЬ. Стратегічна ціль, яку важко досягти, як і відстежити процес. Російська дезінформація формує переконання, цінності та стиль мислення в певній аудиторії. Якщо цільова аудиторія відмовляється від проросійських переконань або навіть заперечує їх, то ціль досягнуто. Виміряти досягнення цілі можна за допомогою проведення соціальних опитувань, фокус-груп та дизайну до/після-тестування.

6 ЗМІНА ПОВЕДІНКИ. Досягнення цієї цілі полягає в тому, що аудиторія починає діяти на підставі власних суджень і перестає бути жертвою російської пропаганди. Таку ціль найважче досягти і ще складніше виміряти, оскільки люди діють поза інформаційним простором. Утім, проведення соціальних опитувань, фокус-груп і дизайну до/після-тестування допоможуть зрозуміти, чи вжиті заходи були вдалими.

ЦІЛІ	ЗАПИТАННЯ	МЕТОДИ ВИМІРЮВАННЯ
ЗАЛУЧЕННЯ ВРАЗЛИВОЇ АУДИТОРІЇ	■ Чи досягли меседжі цільової аудиторії? ■ Якою була реакція? ■ Скільки людей підписалися / відреагували / прочитали? ■ Який канал комунікації був найбільш ефективним? ■ Чи поширилися меседжі за межі цільової аудиторії?	■ Дані ТБ-каналів ■ Дані медіа ■ Протоколи зустрічі ■ Meta Business Suite ■ Twitter Analytics ■ Telegram Analytics ■ YouTube Analytics ■ SimilarWeb ■ Google Analytics
ПОБУДОВА ДОВІРИ	■ Скільки людей підписалися / відреагували / прочитали? ■ Скільки було поширень? ■ Скільки було згадок в інших медіа, соціальних мережах тощо? ■ Як часто організація фігурує в інформаційному просторі?	■ Дані ТБ-каналів ■ Дані медіа ■ Meta Business Suite ■ Twitter Analytics ■ Telegram Analytics ■ YouTube Analytics ■ SimilarWeb ■ Google Analytics ■ Контент-аналіз
ПІДВИЩЕННЯ ОБІЗНАНОСТІ	■ Скількох людей охопили освітні та комунікаційні кампанії? ■ Якою була реакція? ■ Чи засвоїла аудиторія інформацію? ■ Чи стала кампанія частиною суспільного дискурсу?	■ Meta Business Suite ■ Twitter Analytics ■ Telegram Analytics ■ YouTube Analytics ■ SimilarWeb ■ Google Analytics ■ Опитування
ВИБУДОВА СТІЙКОСТІ	■ Скількох людей охопили освітні та комунікаційні кампанії? ■ Якою була реакція? ■ Чи засвоїла аудиторія інформацію? ■ Чи розвинулося критичне мислення?	■ Опитування ■ Анкетування ■ Проведення тестів



ЦІЛІ	ЗАПИТАННЯ	МЕТОДИ ВИМІРЮВАННЯ
ЗМІНА ПЕРЕКОНАНЬ	■ Чи трапилися зміни всередині громади / суспільства? ■ Чи зменшилася довіра до російських каналів комунікації? ■ Чи зменшилася кількість проросійських наративів у середині цільової аудиторії? ■ Чи зменшився негативний вплив російської дезінформації?	■ Опитування ■ Анкетування ■ Соціальні дослідження ■ Фокус-групи ■ Дизайн до/після-тестування
ЗМІНА ПОВЕДІНКИ	■ Чи стала цільова аудиторія діяти інакше ■ Чи втратила російська пропаганда вплив? ■ Чи впала довіра до російських джерел інформації? ■ Чи стали наші меседжі сильнішими, ніж меседжі російської пропаганди?	■ Опитування ■ Анкетування ■ Соціальні дослідження ■ Фокус-групи ■ Дизайн до/після-тестування

Сучасні технології дають змогу відстежувати проміжні результати стратегічних комунікацій і збирати статистичні дані. Наводимо приклади таких інструментів.

GOOGLE ANALYTICS

Надає набір інструментів для вимірювання взаємодії споживачів з рекламними матеріалами, включаючи поведінку на цільових вебсайтах.

META BUSINESS SUITE

Оптимізує облікові записи Facebook та Instagram на одній зручній інформаційній панелі. За допомогою платформи можна керувати всіма обліковими записами, власником чи адміністратором яких є людина, за допомогою різних інструментів, щоб набагато легше контролювати

присутність бренду в соціальних мережах.

TWITTER ANALYTICS

Показує, як аудиторія реагує на контент, які комунікаційні методи та ходи працюють, а які — ні. Ці дані використовуються, щоб оптимізувати майбутні кампанії в Twitter й отримати кращі результати.

YOUTUBE ANALYTICS

Використовується для кращого розуміння ефективності відео та каналу за допомогою ключових показників і звітів у YouTube Studio.
Примітка. Деякі дані, як-от географія, джерела трафіку чи стать, можуть бути обмежені. Також не всі функції працюють на мобільних пристроях.

TELEGRAM ANALYTICS

Одна з багатьох переваг Telegram — вбудовані інструменти аналітики. Канали Telegram мають статистику каналу та багатофункціональну інформаційну панель, яка дозволяє відстежувати зростання аудиторії каналу з плином часу.

SIMILARWEB

Інструмент, що оцінює загальний обсяг трафіку, який отримують різні вебсайти. Це дає змогу побачити найпопулярніші джерела трафіку конкурентів, розбиті на шість основних категорій, включаючи сайти переходів, трафік із соціальних мереж і найпопулярніші ключові слова пошуку.

Окрім цього, можна користуватися інформацією, зібраною за допомогою різних інструментів соціальних досліджень, таких як **ФОКУС-ГРУПИ** та **ДИЗАЙН ДО/ПІСЛЯ-ТЕСТУВАННЯ**.

ФОКУС-ГРУПИ (структуровані обговорення у відібраних малих групах) регулярно використовуються як у дослідженнях ринку, так і комунікаційних кампаніях, щоб викликати глибоку реакцію на продукти, що випробовуються. Цей формат дозволяє дослідникам спостерігати за спонтанними реакціями на підказки та зондувати респондентів на предмет більшої кількості інформації. Це відрізняє **ФОКУС-ГРУПИ** від **ОПИТУВАНЬ**, які можуть бути більш репрезентативними, але покладаються на те, що респонденти обирають однакові та заздалегідь визначені відповіді на питання, які вловлюють менше нюансів. Фокус-групи корисні для збору початкових вражень про низку альтернатив для потенційного змісту комунікаційної кампанії перед масштабуванням заходів для ширшої аудиторії.

Ще одним методом є **ДИЗАЙН ДО/ПІСЛЯ-ТЕСТУВАННЯ**, за яким учасників програми опитують або тестують тим самим набором запитань як до, так і після їх участі в програмі. Наприклад, учасники програми медіаграмотності можуть узяти участь у тестуванні, що пропонує їм відрізнити правдиві новини від неправдивих як до, так і після участі в програмі. Будь-яке підвищення здатності розрізняти правдиві новини від неправдивих свідчить про ефективність програми²².

Це основний, але не повний перелік цілей, запитань та інструментів вимірювання ефективності вжитих комунікаційних заходів. Боротьба з російською дезінформацією — складний і нелінійний процес, тому під кожен окремий випадок потрібно адаптувати як цілі стратегічних комунікацій, так і способи вимірювання прогресу.

Існує [Інтегрована](#) система оцінювання АМЕС, яка забезпечує послідовний і надійний підхід, що підійде для організацій будь-якого розміру і може легко адаптуватися під конкретних користувачів і завдання. Завдяки інструментарію АМЕС можна виміряти ефективність проведеної комунікаційної кампанії, включаючи реакції аудиторії, результати та кінцевий ефект.

²² Complete
Guide. Countering
Disinformation
(Електронний
ресурс)





«БІЛІ СПИСКИ ОФІЦІЙНИХ ТА НАДІЙНИХ ДЖЕРЕЛ ІНФОРМАЦІЇ» ВІД ЦЕНТРУ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА КУЛЬТУРИ ТА ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

Для ефективних стратегічних комунікацій і протидії російській пропаганді, дезінформації та фейкам Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України розробив [«Білий список офіційних та надійних джерел інформації»](#).



Він містить посилання на вебсайти та соціальні мережі таких категорій джерел:

- державні органи влади;
- державні структури;
- представники державних органів влади та державних структур;
- міські голови;
- очільники обласних державних адміністрацій;
- благодійні фонди;
- медійні експертні організації;
- медіа;
- представники медіа та експертних організацій;
- популярні блогери, лідери громадської думки.

Центр стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України також розробив окремий «Білий список офіційних та надійних YouTube-каналів».

Ці списки затверджені та погоджені з такими громадськими організаціями у сфері боротьби з дезінформацією, як:

- Інститут масової інформації;
- Texty.org.ua;
- Інститут інформаційної безпеки;
- Інтерньюз-Україна;
- Детектор медіа.

Джерелам з «білих списків» можна довіряти, проте закликаємо не забувати, що ніхто не застрахований від хакерського зламу навіть офіційних акаунтів, а також комунікаційних помилок і непорозумінь, тож радимо в будь-якому випадку аналізувати, критично осмислювати та перевіряти в інших джерелах усю отриману інформацію, щоб запобігти поширенню дезінформації.

ПЕРЕВІРКА ЗОБРАЖЕНЬ І ВІДЕО НА СПРАВЖНІСТЬ І ВІДСУТНІСТЬ СТОРОННЬОГО ВТРУЧАННЯ ТА РЕДАГУВАННЯ

Якщо новина містить фотографію, її можна перевірити за пошуком в інтернеті. Google має вбудовану функцію перевірки зображень на предмет оригінальності або ж слідів редагування. Так можна побачити, що для зовсім різних новин використовуються одні й ті ж зображення.

ІНСТРУМЕНТИ, які можна використувати для перевірки зображень:

- [RevEye Reverse Image Search](#) — розширення для Chrome;
- [TinEye](#) — перевірка зображення за посиланням;
- [Image Edited?](#) — пошук слідів редагування;
- [FotoForensics](#) — сайт для пошуку слідів редагування та встановлення даних про зображення;
- [Who stole my pictures](#) — плагін для Mozilla Firefox.

НА ЩО ВАРТО ЗВЕРНУТИ УВАГУ, коли ви знайшли першоджерело фотографії?

ДАТИ ПУБЛІКАЦІЙ: однакові чи різні?
МІСЦЕ ПУБЛІКАЦІЙ: хто опублікував це фото, чи можна довіряти цьому джерелу?
ЧИ ВІДПОВІДАЄ НАЗВА та зміст статті фотографії?
ЧИ Є ВІДМІННОСТІ між оригіналом, який ви знайшли, і фото, яке ви хотіли перевірити? Наприклад, фото обрізане, додані або змінені елементи.
У ЯКІЙ КРАЇНІ ЗРОБЛЕНЕ ФОТО? Про яку країну йдеться в новині?

**ЯК АНАЛІЗУВАТИ ВІДЕО
НА ПРЕДМЕТ ПРАВДИВОСТІ?**

УВАЖНО ПЕРЕГЛЯДАТИ ДАНІ про це відео (дата публікації, інформація про канал, на якому воно розміщене, інші відео автора тощо).

ПЕРЕГЛЯДАТИ КОМЕНТАРІ до відеоролика. Дуже часто коментатори дають посилання на першоджерело або інші важливі деталі, що свідчать про неправдивість інформації.

ПІД ЧАС ПЕРЕГЛЯДУ ЗРОБИТИ ЗНІМОК ЕКРАНА та перевірити за пошуком зображень у Google.

ЗВЕРНУТИ УВАГУ НА КАДРУВАННЯ, наявність логотипа на відео, а також на те, що зображене на відео: дорожні знаки, назви вулиць, пора року.

ПРОАНАЛІЗУВАТИ, чи відповідає назва відео його змісту.

[«Детектор медіа»](#) та [«StopFake»](#) у своїх статтях детально описали, яким чином виявляти й спростовувати фото- та відеофейки, а також як знаходити вже видалені вебсторінки. Радимо з ними ознайомитися.

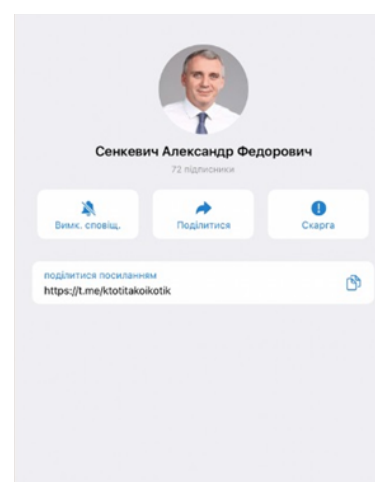
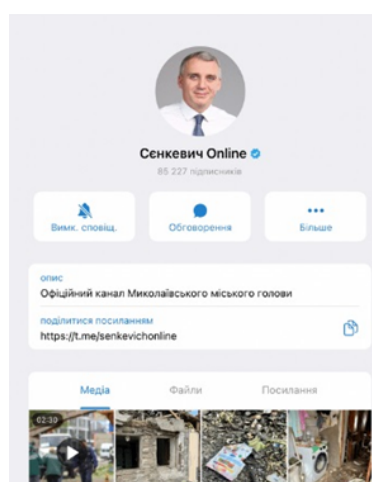


ЯК ВІДРІЗНИТИ СПРАВЖНІЙ ОБЛІКОВИЙ ЗАПИС У СОЦМЕРЕЖАХ ВІД ПІДРОБЛЕНОГО?

Російські пропагандисти дуже часто використовують технологію підроблених профілів у соцмережах українських політиків, військових, органів державної влади, силових структур тощо. Несправжні профілі поширюють дезінформаційні наративи та фейки.

ІСНУЄ КІЛЬКА МАРКЕРІВ, ЩО СВІДЧАТЬ ПРО СПРАВЖНІСТЬ ОБЛІКОВОГО ЗАПИСУ:

- верифікаційний значок (синя галочка);
- написання імені і username (часто наявні помилки, інші символи, ніж кирилиця чи латиниця);
- кількість підписників (у справжніх профілів вона зазвичай вища);
- кількість публікацій (вік облікового запису);

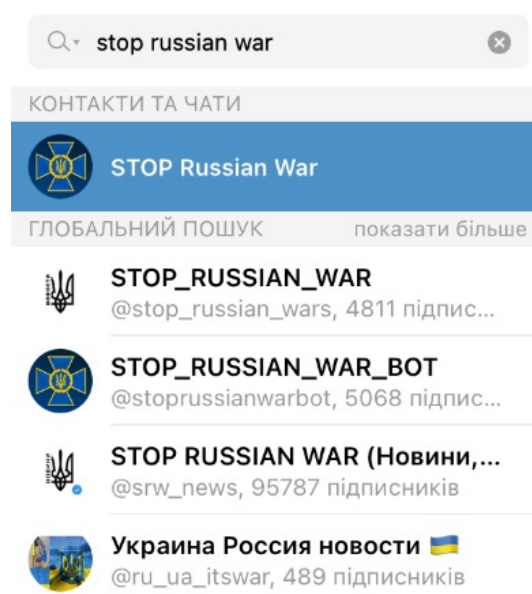


- згадка про нього в інших джерелах;
- адекватність контенту;
- кількість ідентичних сторінок.

ПЕРЕВІРКА ЧАТБОТІВ НА СПРАВЖНІСТЬ. У ЧОМУ НЕБЕЗПЕКА ФЕЙКОВИХ ЧАТБОТІВ?

Під час пошуку чатбота завжди краще переходити на нього за посиланням, розміщеним на офіційних верифікованих джерелах, адже кількість схожих фейкових ботів дуже велика. Чатботи інколи навіть більш шкідливі, ніж фейкові сторінки органів влади, адже вони створені для збору даних. Людина може стати жертвою шахраїв, а якщо проживає на тимчасово окупованих територіях, то фейковий чатбот

буде небезпечним для життя, якщо її персональні дані потраплять до рук російських спецслужб.



ЯК ПОСКАРЖИТИСЯ НА НЕСПРАВЖНІ ОБЛІКОВІ ЗАПИСИ ТА ДОПИСИ, ЩО МІСТЯТЬ НЕПРАВДИВУ ІНФОРМАЦІЮ, У СОЦМЕРЕЖАХ?

FACEBOOK

У разі виявлення контенту та/або облікових записів Facebook, що поширюють шкідливий контент, потрібно перейти за посиланнями, наведеними нижче:

■ [позначити публікацію Facebook як неправдиву новину](#);

■ [повідомити про порушення](#);

■ якщо це реклама — перейти в [бібліотеку реклами](#) й поскаржитися на неї там.

Звернення можуть бути направлені до Наглядової ради. [Вона виконує роль зовнішнього апеляційного органу](#) в разі відмови в задоволенні початкової скарги.

INSTAGRAM

Щоб поскаржитися на шкідливу дезінформацію або мізінформацію, потрібно перейти на сторінку [«Зменшення поширення неправдивої інформації»](#) в Instagram.

FACEBOOK MESSENGER

Щоб поскаржитися на вже наявний діалог, потрібно в меню справа від діалогу натиснути кнопку «Поскаржитись». Також там є опції «Ігнорувати повідомлення» та «Заблокувати». Управляти запитом на переписку від людей, що не є друзями у Facebook, можна [в меню в розділі «Отримання запитів на переписку»](#).

WHATSAPP

Щоб повідомити про шкідливий вміст у WhatsApp, [потрібно виконати наведені тут інструкції](#). Варто зауважити, що WhatsApp — це закрита зашифрована

програма обміну повідомленнями, тому моніторинг контенту в цій програмі відрізняється від інших соціальних мереж і платформ, перелічених вище.

GOOGLE

Різні продукти Google мають власні умови використання, які містять обмеження щодо мови ненависті, оманливої поведінки, контенту, а також способи повідомлення про неправдиву інформацію та інший шкідливий контент. Однак пошуковик Google — найбільш релевантний у випадку цього посібника. Інструмент для запиту на видалення інформації з пошуку Google [можна знайти на цій сторінці](#).

TIKTOK

Щоб повідомити про відео, коментар, користувача, хештег тощо, які підозрюються в неправдивій інформації та іншому шкідливому вмісті, варто переглянути детальні інструкції в розділі [«Повідомити про проблему»](#).

TWITTER

Щоб повідомити про твіти, списки та особисті повідомлення, які поширюють шкідливий контент, потрібно дотримуватися [інструкцій, наведених тут](#). Twitter визначає шкідливий контент у своїх [«Правилах Twitter»](#), які можуть допомогти користувачу зрозуміти, що заборонено і може бути оскаржено²³.

²³ Combating Information Manipulation: A Playbook for Elections and Beyond (Електронний ресурс)





СПИСОК ФАКТЧЕКІНГОВИХ СЕРВІСІВ В УКРАЇНІ ТА ЗА КОРДОНОМ, ЯКІ МИ РЕКОМЕНДУЄМО ВИКОРИСТОВУВАТИ, ОПИС ЇХ ФУНКЦІОНАЛА ТА ОСОБЛИВОСТЕЙ

ЦЕНТР СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА КУЛЬТУРИ ТА ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ створений у березні 2021 року. Робота Центру сфокусована на протидії зовнішнім загрозам, об'єднанні зусиль держави та громадських організацій у боротьбі з дезінформацією, оперативному реагуванні на фейки, а також промоції українських наративів. Центр активно навчає державних службовців і працівників поліції ефективно протидіяти фейкам і російській дезінформації, інформує громадян України та міжнародних партнерів про інформаційні загрози й наративи ворожої пропаганди.

«VOXCHECK» — фактчекерський проєкт від **«VoxUkraine»**. Заснований у січні 2016 року. Спочатку спеціалізувався на аналізі брехні та маніпуляцій українських політиків, проте після початку повномасштабної війни почав спростовувати російські фейки, готувати аналітичні статті про російські гібридні інформаційні загрози.

«STOPFAKE» — фактчекерський проєкт, який працює на базі **Могилянської школи журналістики** з березня 2014 року. Ініціатива спростовує окремі фейки, продукує ґрунтовні аналітичні статті, дайджести російської дезінформації та дослідження, а також підготувала чимало навчальних матеріалів про те, як розпізнавати фейки. Платформа доступна аж 13 мовами світу.

«TEXTY.ORG.UA». Агенція журналістики даних **«Texty.org.ua»** заснована у 2010 році. Головною відмінністю від інших медіа є її спрямованість на **аналіз, опрацювання та візуалізацію великих масивів даних під час написання журналістських репортажів**. Оперує конкретними цифрами та фактами, що дозволяє вважати її матеріали такими, що заслуговують на довіру. **«Тексти» регулярно публікують дайджести російської дезінформації на основі машинного аналізу пропагандистських сайтів**. Вони зручно розбиті за наративами. Ще одним цікавим інструментом є **база псевдосоціологів і прихованих піарників**, яка дозволяє швидко зрозуміти надійність експертної думки в новині.

Агенція розробила додатки для браузерів Google Chrome та Mozilla Firefox, а також чатбот у телеграмі під назвою **«Фейкогриз»**. Він уміє визначати ненадійні сайти та дезінформацію. Працює за допомогою позначень від користувачів, а також нейронної мережі, розробленої спеціалістами «Текстів». Ефективний для дослідників у сфері протидії дезінформації, дозволяє створювати масиви даних і таблиці з неправдивими новинами.

«ДЕТЕКТОР МЕДІА». Фактчекерська ініціатива однойменної громадської організації збирає базу як власних спростувань російських фейків, так і інших фактчекерських організацій. Також готує дайджести російської

пропаганди та аналітичні статті. Цікавий спецпроект [«МедіаЧек»](#), де аналізується дотримання українськими медіа журналістських стандартів та етики. Також журналісти створили [«Дошку ганьби»](#) політиків і медійників, що відкрито підтримали російську агресію проти України. Сайт має кілька інших цікавих спецпроектів, більшість з яких, зокрема, присвячені темі війни та російської дезінформації. Ще один цікавий проєкт, спрямований на підвищення рівня медіаграмотності, — [«Медіа Драйвер»](#).

Нещодавно організація запустила новий проєкт — [«#DisinfoChronicle»](#), де зібрані спростування фейків, маніпуляцій і брехні російської пропаганди. Є можливість пошуку та сортування за датами й тегами.

[«БЕЗБРЕХНІ»](#). Фактчекерська ініціатива [«БезБрехні»](#) відрізняється справді ґрунтовним і глибоким аналізом фейків і їх детальним і якісним спростуванням. Також фактчекери створили кілька методичних посібників і навчальних статей на тему перевірки інформації. Мають розгалужену регіональну мережу місцевих фактчекінгових ініціатив, з якими тісно співпрацюють.

[УКРАЇНСЬКИЙ КРИЗОВИЙ МЕДІА-ЦЕНТР](#) має у своєму складі [групу з аналізу гібридних загроз](#), що аналізує російські інформаційні загрози та виробляє шляхи їх подолання,

які подає у своїх аналітичних матеріалах.

[«ЯК НЕ СТАТИ ОВОЧЕМ»](#) — проєкт відомої фактчекерки Оксани Мороз. Він не лише спростовує російські фейки та дезінформацію, а й має просвітницьку мету — виховання інформаційної гігієни та медіаграмотності в українців. Проєкт разом із сервісом [«Youcontrol»](#) створив цікавий інструмент — [базу даних російських пропагандистів](#).

[«GWARA MEDIA»](#) — медіа з Харкова, що активно протидіє фейкам і дезінформації. Журналісти готують дайджести російської дезінформації, аналітичні статті та спростування окремих фейків.

[«EU VS DISINFORMATION»](#). Офіційний проєкт Європейського Союзу з протидії фейкам і дезінформації. Містить [базу даних російської дезінформації](#), яка складається зі спростувань фейків не лише щодо України, а й Білорусі та інших країн Східного Партнерства. На сайті представлено чимало аналітичних статей і наукових досліджень у сфері протидії дезінформації. Також є інтерактивні ігри та вікторини, спрямовані на підвищення рівня медіаграмотності населення Європейського Союзу і країн Східного Партнерства. Сайт працює 15 мовами.

[«BELLINGCAT»](#) — відома у світі агенція журналістських розслідувань на основі відкритих даних (методом OSINT). Боротьба з фейками та дезін-



формацією не є її головним завданням, проте вона успішно справляється і з цим напрямом.

«INFORMNAPALM» — міжнародна розслідувальна спільнота, заснована після початку російської агресії проти України у 2014 році. Об'єднала волонтерів з понад 20 країн, які проводять OSINT-дослідження, перекладають і поширюють публікації іноземними мовами, ведуть важливу медійну, дипломатичну й просвітницьку роботу. Розслідування спільноти з ідентифікацією російських військово-службовців, формувань і військової техніки, зібрані протягом гібридного етапу війни (2014–2022 рр.), оформлені в зручні для користування бази даних, які відіграли важливу роль у доведенні факту російської агресії.

«MYTHDETECTOR» — грузинський фактчекінговий сервіс, заснований у 2014 році Фондом розвитку медіа, спрямований на боротьбу з російськими фейками й дезінформацією. Містить базу даних перевірки фактів.

«START2THINK» — польський портал, що має дуже цікаву та різноманітну підбірку різних сервісів та інструментів, які стануть у пригоді для перевірки не лише текстового, а й аудіо- та відеоконтенту.

«POLYGRAPH» — американський професійний фактчекінговий сервіс, що

спростовує російські фейки та дезінформацію.

Для перевірки новин на правдивість також використовуються різні інструменти із застосуванням штучного інтелекту. Спеціалістами **«Gwara Media»** було розроблено **телеграм-бот «Перевірка»**. Командою Центру стратегічних комунікацій та інформаційної безпеки було створено **інструмент для перевірки ботів**. Для перевірки інформації потрібно завантажити відповідний контент у бот і протягом кількох хвилин отримати відповідь про правдивість інформації.

Окрім профільних фактчекерських державних інституцій, а також громадських ініціатив, спростуванням російських фейків і дезінформації ситуативно займаються й інші органи. Переважно це структури, що працюють у сфері національної безпеки та оборони: **Рада національної безпеки і оборони України, Служба безпеки України, Міністерство оборони України, Генеральний штаб ЗСУ, Державна служба спеціального зв'язку та захисту інформації України** тощо. Неправдиву інформацію також подекуди спростовують міністерства, обласні державні адміністрації та органи місцевого самоврядування (якщо інформація профільна для них), хоча загалом вони мають інші функції і протидіють дезінформації лише ситуативно, коли цього потребують обставини.

ІНСТРУМЕНТИ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ (OSINT) ДЛЯ ІДЕНТИФІКАЦІЇ ІНФОРМАЦІЙНИХ МАНІПУЛЯЦІЙ

OSINT — це збір та аналіз інформації з публічних (відкритих) джерел. Ці ресурси можна використовувати для відстеження та виявлення дезінформації.

НАБІР ОНЛАЙН-РОЗСЛІДУВАНЬ «BELLINGCAT»

Цей гугл-документ зі зручною навігацією містить вкладки для різних інструментів перевірки інформації, як-от перевірка зображень і відео; контент та акаунти в соціальних мережах; телефонні номери та закриті служби обміну повідомленнями; карти та послуги на основі місця перебування; транспортні трекери; аналіз IP-адрес і вебсайтів; міжнародні компанії; навколишнє середовище; інструменти для поліпшення онлайн-безпеки, конфіденційності та візуалізації даних; академічні ресурси; додаткові посібники.

ПОСІБНИК ДЛЯ ПЕРЕВІРКИ МЕДІА

на предмет дезінформації та маніпуляцій на основі журналістики даних. Ця книга допоможе проводити OSINT-дослідження облікових записів у соціальних мережах, виявляти ботів і маніпуляції зображеннями. Вона також містить ресурси для розслідувань в інтернеті й поради та інструменти для атрибуції.

ПОСІБНИК 3 МЕДІАМОНІТОРИНГУ

ПРОЄКТУ «BEACON». Допоможе проаналізувати наративи дезінформації та їх джерела на основі даних. Посібник — чудова стартова точка для дослідників, зацікавлених у проведенні

медіамоніторингу, але невпевнених, з чого почати, а також для тих, хто хоче переконатися, що застосовує найкращі методологічні практики.

ІНСТРУМЕНТ «CROWDTANGLE»

Facebook створив «CrowdTangle» як інструмент для виявлення та моніторингу трендів у соціальних мережах. Інструмент може відстежувати перевірені облікові записи, сторінки та публічні групи. Його також можна використовувати для моніторингу загальнодоступних облікових записів в Instagram і розділів subreddit на платформі «Reddit».

СПИСОК РЕСУРСІВ ДЛЯ БОРОТЬБИ З ІНФОРМАЦІЙНИМИ МАНІПУЛЯЦІЯМИ «ANNEX»

У ньому представлений широкий набір інструментів для протидії дезінформації, медіамоніторингу, аналізу соціальних мереж тощо від провідних міжнародних організацій.

При цьому потрібно розуміти, що контекст кожної комунікаційної кампанії, організації та країни відрізнятиметься й потребуватиме поєднання інструментів, навичок і партнерів, тому добре знання інструментів, які можуть допомогти ідентифікувати та контролювати поточні кампанії, дозволить давати адекватну відповідь і розвивати стійкість до дезінформації та маніпуляцій.



ДЕЯКІ ПОРАДИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ЗАХИЩЕНІ БРАУЗЕРИ

Захищені веббраузери містять додаткові протоколи безпеки, що допомагають запобігти несанкціонованій діяльності третіх сторін під час користування інтернетом. Ці браузери блокують функції та дії, яких немає в попередньо затвердженому «білому списку» авторизованих програм і дій (наприклад, реклама, відстеження історії перегляду тощо).

1 BRAVE — це швидкий, безкоштовний, безпечний веббраузер для мобільних і комп'ютерних пристроїв. За замовчуванням Brave містить вбудовані блокувальники реклами, запобігає будь-якому відстеженню вебактивності користувачів, оптимізує термін служби акумулятора мобільного пристрою та використовує менше ресурсів даних (тому дуже швидко завантажує сторінки). Закладки та інші налаштування зі старого браузера користувача можна легко імпортувати в Brave. Він працює на Android, iOS, Windows 10, MacOS або Linux.

2 VIVALDI не відстежує історію перегляду користувачів або користувацькі дані, а його блокувальник трекерів блокує рекламу та сторонні вебтрекери. Він також містить за замовчуванням кілька приватних пошукових систем (включаючи DuckDuckGo, StartPage, Neeva і Qwant). Синхронізація пристрою зашифрована. Vivaldi також пропо-



нує широкий спектр інструментів для навігації та налаштування інтерфейсу, які забезпечують зручний користувацький досвід. Vivaldi працює на MacOS, Linux, Windows і Android.

ЗАХИЩЕНА ЕЛЕКТРОННА ПОШТА

Це служби електронної пошти, для яких додаткові функції безпеки більш пріоритетні, ніж користувацький досвід. Такі сервіси шифрують

листи з електронної пошти на файловому рівні як під час надсилання, так і збереження на вебсерверах. Багато з них також мають безліч інших функцій конфіденційності та безпеки.

PROTONMAIL пропонує наскрізне шифрування електронної пошти на основі ключів RSA, які використовуються для облікового запису ProtonMail користувача. За допомогою цього типу шифрування лише користувач облікового запису Protonmail й одержувач листа можуть переглядати або отримувати доступ до повідомлень, а треті сторони (включаючи ProtonMail) — ні. ProtonMail також захищений на апаратному рівні центрів обробки даних, які розташовані в ядерному бункері з повністю зашифрованими жорсткими дисками на кожному сервері. Доступний через вебпошту, мобільні додатки та Tor, ProtonMail має зручний інтерфейс й опції антицензури (отримання доступу попри блокування урядом).

БЕЗПЕЧНІ МЕСЕНДЖЕРИ

Безпечні месенджери пропонують наскрізне шифрування для спілкування користувачів. Воно не дозволяє відстежувати будь-які дані, які надсилаються через ці платформи (включно з будь-якими серверами, на яких розміщені дані), тому лише співрозмовники побачать або отримують доступ до інформації.

1 SIGNAL — це програма для обміну повідомленнями з відкритим кодом. І відправник, і одержувач повинні зареєструвати обліковий запис у Signal, ви-

користовуючи номер мобільного телефону (Signal не зберігає і не передає номер телефону користувача). Програма не витягує інформацію зі списків контактів телефону і не має доступу до реєстраційних даних користувача. Signal пропонує опцію автоматичного знищення всіх комунікацій (дзвінків і повідомлень), а також дозволяє користувачам «ретранслювати виклики» через сервер Signal, щоб уникнути розкриття IP-адреси. Signal має опцію групових відеодзвінків до 40 осіб і чатгрупи до 1 000 учасників. Працює на настільних комп'ютерах, мобільних телефонах і планшетах з операційними системами Android, Apple, Windows і Linux. Signal має понад 40 мільйонів активних облікових записів, активну спільноту підтримки та самофінансується як засновниками-активістами, так і іншими спонсорами.

2 WICKR — це комерційний месенджер, який дозволяє користувачам безпечно надсилати та отримувати повідомлення, зображення, відео, аудіо та файли. І відправник, і одержувач повинні мати Wickr для спілкування, але ви можете знайти свого «друга», не завантажуючи або синхронізуючи Wickr зі списком контактів вашого телефону. Він надсилає окремий ключ шифрування для кожного повідомлення, який отримує тільки одержувач (Wickr також не має доступу до нього). Wickr пропонує широкі можливості керування, і відправник може вказати, як довго одержувач буде бачити або зберігати дані. Відправник також може налаштувати різні рівні дозволів для осіб, яких запрошує безпосередньо до своєї мережі, порівняно з іншими номерами, які розглядає як «поза мережею».



ЦЕНТР СТРАТЕГІЧНИХ
КОМУНІКАЦІЙ
ТА ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ



ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА



Швеція
Sverige