ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ: РЕГІОНАЛЬНИЙ ВИМІР

Методичні рекомендації для регіональних медіа та місцевих органів влади

USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ · ЄДНАННЯ · УНЦПД · ЦЕНТР ДЕМОКРАТІЇ ТА ВЕРХОВЕНСТВА ПРАВА · VOX CHECK · ЦЕНТР ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

Цей посібник створено ГО «Вокс Україна» та Центром протидії дезінформації за підтримки ICAP Єднання у межах проєкту «Ініціатива секторальної підтримки громадянського суспільства України», що реалізується ICAP Єднання у консорціумі з Українським незалежним центром політичних досліджень (УНЦПД) та Центром демократії та верховенства права (ЦЕДЕМ) завдяки щирій підтримці американського народу, наданій через Агентство США з міжнародного розвитку. Зміст (указати вид публікації) не обов'язково відображає погляди ICAP Єднання, погляди Агентства США з міжнародного розвитку або Уряду США.

USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

ЄДНАННЯ

УНЦПД

ЦЕНТР ДЕМОКРАТІЇ ТА ВЕРХОВЕНСТВА ПРАВА

VOX CHECK

ЦЕНТР ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

МЕТА СТВОРЕННЯ РЕКОМЕНДАЦІЙНОГО МАТЕРІАЛУ

На створення та поширення ворожої пропаганди щодня витрачають мільйони доларів. І мова йде не лише про зомбування їхніх аудиторій “глубінного народа” публічними пропагандистами. На жаль, найчастіше ми бачимо лише вершину айсберга російської пропаганди та дезінформації, для багатьох із нас – це недолугі дурниці, яка українцям, як то кажуть, на голову не налазять, а от московити їх споживають з радістю, адже роль подібних пропагандистських казочок – підгодовувати росіянське “вєлічіє” та ганити “західний світ” та українців.

Утім, російська пропаганда та дезінформаційна діяльність у багатьох випадках є значно небезпечнішою для нас, ніж ця видима “вершина айсберга”. Адже росія діє “вітчизняною пропагандою” на власні аудиторії, а для українців та “вестернів”, тобто західних аудиторій, має інші, часом значно тонші методи. Але – і ці методи можливо розкрити, вирахувати, та зупинити їхню ганебну, і часто руйнівну дію. І ми в цьому методичному посібнику – покажемо, як це зробити, дамо приклади, роз’яснимо неочевидне на перший погляд.

Адже ми свідомі того, що працівники органів місцевої влади та регіональні журналісти – це місцеві лідери думок. І саме від вас багато в чому залежить інформаційна безпека вашої громади. Водночас – якими б переконливими знаннями та перевіреними методами не володіли працівники РНБО та громадські організації, які суттєво сприяють протидії дезінформації – без підтримки місцевих еліт з цією напастю боротися дійсно нелегко.

росія атакує нас не лише на полі бою, не лише руйнує наші мирні міста, селища та села, забираючи життя мирних мешканців України. На жаль, суттєвої шкоди завдають і пропагандистські кампанії, які можуть мати різноманітні, як тактичні, так і стратегічні цілі. Але ключовою метою росії на цьому дуже чутливому та для багатьох туманному інформаційному фронті є така: демотивувати українців, психологічно нас зламати, порушити нашу єдність, завадити нам перемогти у війні.

Для досягнення цієї мети росія цілеспрямовано впроваджує в інформаційний простір власні наративи, тобто групи меседжів, які переслідують якусь крупну мету, або ж закладають якусь глобальну, руйнівну для нас ідею. Ці наративи розповсюджують не лише “лайливі голови” на російських екранах, не лише “куплені” журналісти на кшталт Такера Карлсона та інші спокушені ворогом лідери думок. На жаль, росія має ресурси на те, щоби технічними методами “розганяти” фейки, дезінформацію, пропаганду в наших соціальних мережах та месенджерах – від Twitter Facebook, де нерідко є сторінки місцевої влади та місцевих ЗМІ, і аж до будинкових чатів ОСББ та шкільних груп. На жаль, навіть у такі нібито безпечні цифрові середовища також може проникнути ворог, і нашкодити: такі випадки були непоодинокими.

Саме тому ми покладаємося на регіональних інформаційних лідерів та ваші команди. Адже ваша вчасна реакція, ваше вміння побачити, проаналізувати та знешкодити інформаційну загрозу від росії – це наша конкурентна

перевага перед ворогом. Ми свідомі того, що громадський сектор та регіональні лідери, об'єднавши спільні зусилля з центральною владою, і зокрема Центром протидії дезінформації РНБО, ми здатні досягти дуже вагомих цілей. Тобто – суттєвого підвищення інформаційної безпеки в Україні, злагодженішої реакції на фейки та пропаганду росії, більше контролю над безпекою локальних інформаційних середовищ – зокрема, важливих, і досяжних лише для лідерів думок у регіонах. Мова йде про місцеві групи в соціальних мережах та месенджерах, крупні чати локального рівня від 1000 осіб, зрештою – коментарі на офіційних сторінках органів влади та ЗМІ на різних цифрових платформах.

Утім, тут є й дуже хороша новина: Україна ефективно вчиться протистояти російським фейкам та дезінформації, як то кажуть, просто на полі бою. Тобто ми знаходимо способи по-новому реагувати на нові інформаційні загрози. Саме тому Центр протидії дезінформації РНБО та проєкт VoxCheck громадської організації "Вокс Україна" в рамках партнерства з ICAP Єднання розробили ці методичні рекомендації для регіональних лідерів думок, і передовсім – локальних ЗМІ та місцевих органів влади. У посібнику зібрані необхідні інструменти для аналізу та перевірки фактів, розглянуто основні прийоми російської пропаганди та запропоновано алгоритм дій, як їм протидіяти.

ЯК КОРИСТУВАТИСЬ МАТЕРІАЛОМ

Спершу радимо уважно прочитати цей матеріал від початку й до кінця, адже його логіка дуже проста, однак кількість видів та прикладів російського фейкоробства та розповсюдження дезінформації вас може неприємно здивувати. Утім, не варто панікувати: після прочитання ви точно знатимете, як вам діяти, щоб допомогти Україні подбати про власну інформаційну безпеку.

Спершу ми з'ясуємо, чи однаково розуміємо ключові терміни, що стосуються сфери опору російські дезінформації та пропаганді. Далі ми розглянемо ключові соціальні мережі, в яких росія "розганяє" свою дезінформацію, спрямовану на українців. Акцент ми робитимемо саме на регіональному інформаційному аспекті, адже робимо посібник саме для вас – регіональних лідерів думок. Тому ми звертаємо увагу на ті наче й слабко доступні для моніторингу, утім, на жаль, важливі для російських агентів впливу регіональні майданчики.

На наступному етапі ми перейдемо до розгляду тих механізмів впливу, які застосовує росія в українському інформаційному просторі. Що важливо – ми наведемо різні приклади, щоби розкрити повніше ці механізми, щоби вони стали для вас очевидними. Ціль цього розділу – щоби ви могли вирізняти подібні, але вже новіші російські фейки, ботів, випадків "інформаційного алібі" та інші підступні механізми негативного впливу на українську інформаційну безпеку.

Наступний розділ нашого посібника стосується конкретних механізмів фактчекінгу, тобто – перевірки підозрілої інформації, яка – на вашу думку – може шкодити інформаційній, або й фізичній безпеці українців. Експерти Центру протидії дезінформації РНБО та VoxCheck докладно пояснюють, які базові дії слід здійснити, щоби встановити правдивість інформації, зокрема, фото- та відео-матеріалів, щоб проаналізувати ключові соцмережі та медіаресурси.

Зрештою, заключний розділ посібника з методичкими рекомендаціями дасть вам алгоритм, що дозволить ефективно реагувати на інформаційні загрози на регіональному рівні. Відповідальні особи у місцевих органах влади, а також регіональні журналісти, керуючись цими методичними вказівками та користуючись зручними схемами аналізу інформації, зможуть оцінити ситуацію, правильним чином прокомунікувати її з аудиторіями та вплинути на саму загрозу.

Крім того, не варто забувати, що матеріали цього посібника мають стати частиною вашої комунікації з іншими аудиторіями, які можуть контролювати інформаційну безпеку в локальних спільнотах: головами правлінь ОСББ, лідерами місцевих громадських організацій, лідерами місцевих крупних груп у соціальних мережах тощо. Адже ми мусимо щомиті пам'ятати: нині триває визвольна війна українського народу. Наша незалежність і самобутність – під загрозою. І наш ворог сумлінно працює, щоби загроза ця зростала. Тож ми маємо працювати у відповідь, щоб відбити його інформаційні атаки та очистити український інфопростір від фейків та дезінформації.

1/ ОСНОВНІ ТЕРМІНИ

Меседж – окрема одиниця інформації, що передається джерелом для використання кінцевим споживачем або групою таких споживачів. Меседж може бути доставлено різними способами, включаючи фізичний (поштовий лист), вербальний (заява, розмова, дзвінок), електронний (публікація в ЗМІ чи соцмережах) тощо.

Наратив – спосіб подачі або розуміння ситуації чи серії подій, який відображає та просуває певну точку зору чи набір цінностей. Декілька наративів можуть бути об'єднані у гранд наратив.

Гранд наратив – контентний елемент інформаційної та пропагандистської діяльності держави, на утвердження якого спрямовується діяльність комунікативних можливостей держави (публічної дипломатії, зв'язків із громадськістю тощо) у внутрішніх та зовнішніх цільових аудиторіях. Термін позначає переконливу сюжетну лінію, яка аргументовано пояснює події і формується на підставі існуючих у суспільстві уявлень і цінностей.

Маніпуляція — інформація, що має стосунок до реальності, на вигляд правдива, однак свідомо викривлена з метою впливу на реципієнта. Маніпуляціями в публічному просторі користуються для того, щоб попри бажання реципієнта, який сприймає інформацію, нав'язати певні наративи як істинні, або ж сформувати певну модель поведінки чи спонукати до вчинення певної дії. Наприклад, російська пропаганда маніпулює асоціацією "Україна = Окраїна [Польщі або Московії]" виходячи суто із "народної етимології" подібності цих слів. Однак серйозні вчені, філологи та історики, пояснюють, що в слов'янських мовах доречніше було би асоціювати слово "Україна" зі словами "Край", "Країна", "У країні [як єдності]", "Крайна" (в деякий слав'янських мовах). Тобто росіяни маніпулятивно використовують фонетичну та семантичну подібність слів, ігноруючи наукові пояснення.

Фейк — підробка або імітація елементів інформаційного простору: підміна фактів у інформаційному повідомленні, спотворення зображень або відео з метою введення в оману глядачів тощо. Також фейком може бути підробка під канал поширення інформації – банальні боти, які "розганяють" ворожі або деструктивні меседжі, а також більш небезпечні імітації: сторінки ча акаунти ЗМІ, яким довіряє аудиторія, політиків чи лідерів думок, або навіть сторінки міністерств чи регіональних структур. Регіональним лідерам думок варто моніторити як власні бренди, так і загалом присутність регіонально маркованої інфорації в соціальних мережах та основних інформаційних каналах. Якщо ви виявляєте фейкові сторінки, пов'язані з вашим регіоном або публічними особами, варто повідомляти про них на зворотній зв'язок ЦПД РНБО. Про інформаційні фейки (фото, відео, текстові блоки) більше читайте на сторінках цього посібника.

Дезінформація — неправдива чи маніпулятивна інформація, яку навмисно поширюють за допомогою агентів впливу, підконтрольних каналів та структур, щоб ввести в оману реципієнтів (глядачів, слухачів, читачів) стосовно справжнього стану справ, аби створити "викривлену" реальність у їхньому сприйнятті. Приклади класичної дезінформаційної кампанії – тотальне заперечення російською федерацією та її агентами впливу факту причетності росії до збиття літака рейсу М17, попри абсолютну подальшу доведеність цього у суді, а також маніпулятивна кампанія щодо "постановочності звірств росіян у Бучі" із застосуванням широкого спектру фейків, спотворень фото- та відео-матеріалів тощо.

ІПСО (інформаційно-психологічна операція) — заздалегідь підготовлений акт інформаційного впливу на таргетовану (конкретну, свідомо обрану) аудиторію, націлений на досягнення тактичних (паніка, розгубленість, страх) або стратегічних (недовіра, розчарування, апатія) цілей. Зазвичай проходить у короткий проміжок часу. ІПСО є військовою

операцією, попри те, що на перший погляд не застосовує зброї. Однак за допомогою ІПСО ворог може коригувати цілі своїх ракетних та інших ударів, може переконувати "потенційних агентів" у співпраці. Тобто ІПСО також загрожує смертями тисячам українців, попри враження, що це лише "діється у віртуальній реальності". Суттю ІПСО є інформаційний вплив на емоційно-психічний стан мас людей, певних аудиторій. Наприклад, ІПСО через регіональні канали в соціальних мережах можуть проводитися щодо мешканців прифронтових територій. Якщо ви помічаєте наративи, які розхитують психологічну стійкість українців у вашому регіоні, а тим паче якщо такі наративи є постійно повторюваними, і надходять у вигляді схожих меседжів від різних джерел інформації – цілком можливо, що це і є масована ІПСО. У такому разі варто діяти по методиці, описані далі в посібнику, і ніколи не буде зайвим залишити фідбек на одному з каналів зворотного зв'язку ЦПД РНБО.

Місінформація — неправдива інформація, що поширюється без злочинного умислу або наміру ввести в оману. Наприклад, це можуть бути журналістські помилки, чутки та плітки. Утім, усе це може стати основою для створення фейку. І водночас, місінформація може бути додатковим "туманним" тлом для поширення пов'язаних фейків. Прикладом місінформації може бути очорнення публічних осіб через розкручування скандальних чуток довкола них. У цьому випадку місінформація буде супроводжуватися малінформацією, і все разом може бути "чорним піаром", на основі якого до репутації людини "приліплять" фейки. На жаль, це може стосуватися й регіональних лідерів думок.

Маліформація — свідома публікація приватної чи чутливої інформації з метою зашкодити суб'єкту. По суті, це можна вважати "зливом компромату", який при пильному розгляді не має "складу серйозного злочину", однак може додати негативної конотації об'єкту малінформаційної кампанії. Прикладами таких кампаній можуть бути усі, де "певний суб'єкт, схоже, вживає наркотики, зігує, займається любощами з дуже молодими на вигляд людьми тощо". Зазвичай жодного "залізного" доказу злочинної діяльності така інформація не має, однак апелює до стереотипних у суспільстві (або для електорату певного регіону чи політичного спектру) моральних констант. На жаль, наші вороги також використовують малінформацію проти українських можновладців та ключових осіб. Прикладом цього можуть бути маніпуляції довкола "присутності русскіх людєй серед родичів" Головнокомандувача Збройних сил України О.Сирського. Перевірка такої інформації дає приклади цинічного використання родинних зв'язків (парадоксально, але мова йде навіть не про кровну рідню Героя України О. Сирського) для створення образу "непатріотичності" генерала, який, утім, на практиці послідовно доводить свою відданість Україні та нашим цінностям. Якщо ви помічаєте аналогічні кампанії проти регіональних лідерів думок або інституцій – цілком можливо, що і в цьому можуть бути присутні не лише інтереси конкурентів, але й ворожі інтереси. Такі кампанії мають досліджувати фахівці.

Корисні ідіоти — реальні люди, які некритично сприймають інформаційний простір, живуть у полоні московських ілюзій, не дотримуються інформаційної гігієни та схильні несвідомо поширювати меседжі ворожої пропаганди, згенеровані нею фейки, дезінформацію тощо. Походження терміну вказує на те, що люди з некритичним мисленням, політично недалекоглядні ("ідіоти") є водночас корисними для ворожої пропаганди, оскільки й без застосування ботів можуть "розганяти", розповсюджувати меседжі, що є частиною ІПСО або інших інформаційних кампаній ворога. На щастя, боротьба з "корисними ідіотами" може бути ефективною: горе-тіктокери чи інста-блогери, які вибачаються перед українцями за свої недалекоглядні висловлювання. Та й сусідська тітка з Архангельська, яка нині живе в Краматорську, але любить Булгакова з Пушкіним більше від Винниченка з Шевченком, і тому поширює у Facebook дописи, які критикують деколонізацію України – також серед них. З нею завжди можна поділитися відео-контентом про те, як росія використовую "вєлікую культуру" для того, щоб обґрунтовувати, зокрема, намагання окупувати "Русскій город Кієв". Привіт Булгаковолюбам.

2 / ЯК ВИЗНАЧИТИ ВОРОЖІ РЕСУРСИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Цей розділ ми подаємо для того, аби регіональні лідери думок одразу розуміли, де і яким чином ворожа пропаганда та дезінформація може безпосередньо спотворювати регіональний інформаційний простір. Це з одного боку сторінки та акаунти, марковані певним регіоном, що трапляються у соцмережах, з іншого боку – інформаційні кластери (будинкові чати, районні чати, вайбер-сторінки району абощо), до яких можуть інфільтруватися ворожі агенти впливу, які можуть просувати ті або інші наративи ворога. В наступних розділах ми докладніше розповімо про типи маніпуляцій, методи інформаційного впливу, а також покажемо наративи, які просуває ворог через ресурси (соціальні мережі) про які йдеться в цьому розділі.

2.1 / X (TWITTER)

Для визначення неавтентичної сторінки у X (Twitter) зазвичай не потрібні інші ресурси або інструменти. У X (Twitter) є достатньо даних для повного аналізу сторінки. Тому зіткнувшись із поширенням чутливої для вашого регіону інформації з певної сторінки, ви можете перевірити її автентичність.

- Дата створення

За цими даними можна визначити, чи сторінка була створена нещодавно, або завчасно для проведення інформаційної операції.

- Аватар профілю

Зазвичай для ботів та фейкових профілів картинку профілю беруть просто з інтернету. Це надає можливість перевірки картинки через алгоритми розпізнавання зображень:
images.google.com
pimeyes.com
tineye.com

Ці інструменти можуть використовуватися, зокрема, і з метою розпізнавання обличчя за допомогою парсингу всіх світлин, наявних у всесвітній мережі.

Для аналізу підроблених фотографій рекомендується використовувати ресурс:
fotoforensics.com

Цей інструмент надає можливість через компрес фотографії переглянути, які саме ділянки були змінені, де білий колір означає автентичну область, а яскраво виражені райдуги – ділянка у які вносилися корективи.

- Ім'я профілю

В X (Twitter) є два імені профілю, за допомогою яких можна провести детальніший аналіз. Нікнейм (від англ. nickname) – це ім'я, яке автор може змінювати без значних зусиль. Юзернейм (від англ. username) – це ім'я з приставкою «@», зміна якого викликає значні труднощі. Зазвичай боти та фейкові профілі використовують або найтривіальніші комбінації імен та прізвищ, характерних для регіону, або набір символів без конкретного значення.

- Активність

Активність профілю дає значну кількість інформації. Зокрема, це кількість публікацій за певний проміжок часу. Зазвичай велика кількість публікацій в день свідчить про неавтентичність профілю.

- Взаємодія з іншими профілями

Під час аналізу важливо переглянути взаємодію профілю з іншими користувачами. Якщо суб'єкт аналізу активно репостить інформацію інших користувачів, схожих на ботів, або підозрілих ресурсів, найімовірніше профіль оперує в мережі неавтентичної поведінки.

- Мова

Аналізуючи використану мову в публікаціях профілю, через правопис можна зрозуміти, до прикладу, чи використовувався машинний переклад під час написання публікації.

- Загальна інформація профілю

Звичайні користувачі іноді залишають корисну інформацію про себе у шапці профілю. У свою чергу неавтентичні профілі або не залишають інформацію, або використовують сфальсифіковані відомості.

2.2 / TELEGRAM

Telegram за своїм характером не містить великої кількості даних для аналізу, проте використовуючи певні технічні чи логічні особливості існує можливість ідентифікації неавтентичного контенту. В окремих Telegram-каналах можна знайти відкриті коментарі, що дають розуміння того, чи використовуються ним боти. Також потрібно звертати увагу на кількість підписників на каналі та їх співвідношення з переглядами та реакціями на окремі дописи. Канал, який має менш ніж 20% переглядів від загальної кількості підписників, найімовірніше наповнений ботами. Варто також перевіряти автентичність посилання каналу, ворог може створити фейкову сторінку, що імітує оригінальну. В описі каналу зазвичай можна знайти додаткову інформацію, яку залишає автор – це карти, контактні дані, юзернейми адміністраторів, криптогаманці, посилання на інші сайти тощо. Згадана інформація також дуже цінна для аналізу Telegram-каналу.

- **Контент Telegram-каналу**

Перше, на що потрібно звертати увагу при дослідженні Telegram-каналу – це його контентне наповнення. Так, варто зауважувати на наявність у каналі маніпулятивних дописів чи дописів, які містять фейкову інформацію. Якщо такі дописи наяві, необхідно звернути увагу на їхню кількість протягом останнього періоду – якщо подібних публікацій багато (у співвідношенні до іншого контенту), то існує висока ймовірність того, що це джерело є ворожим.
Також варто зважати на загальну конотацію дописів досліджуваного Telegram-каналу. Деколи адміністратори Telegram-каналу підбирають інформацію таким чином, щоб створити загальний негативний новинний фон та нав'язати читачеві відчуття так званої «зради».

- **Опис Telegram-каналу**

Водночас потрібно опрацювати інформацію, розміщену в розділі «Опис». Інколи адміністратори залишають посилання на акаунти зворотнього зв'язку чи інформацію про способи фінансової підтримки Telegram-каналу, включно з даними про банківські реквізити. Вказане може допомогти ідентифікувати адміністраторів досліджуваного Telegram-каналу.

- **Реакції на дописи Telegram-каналу**

Також варто звертати увагу на інформацію стосовно реакцій на дописи досліджуваного Telegram-каналу, особливо у їхньому співвідношенні до загальної кількості його підписників. У разі, якщо перегляди допису складають лише незначний відсоток від загальної кількості підписників Telegram-каналу – це може свідчити про його наповнення ботами. Це ж стосується лайків. Також варто згадати про коментарі під дописами. Якщо вони однотипні або ж взагалі однакові, чи містять помилки не притаманні українській мові, можна зробити висновок, що досліджуваний Telegram-канал використовує ботів для створення ілюзії користувацької активності.

- **Згадування інших Telegram-каналів**

Окремі Telegram-канали залишають різного роду згадування інших Telegram-каналів: прямі посилання, цитати, відсилки тощо. Якщо такі згадування є частими у дописах досліджуваного Telegram-каналу – це може свідчити про існування мережі каналів, у якій він функціонує та публікує контент.

- **Графік опублікування дописів**

Якщо в графіку опублікування дописів досліджуваного Telegram-каналу прослідковується певне системність, наприклад, публікації з'являються кожні 45 хвилин у часовий проміжок з 09:00 до 17:00, це може свідчити про неавтентичність такого каналу.

- **Присутність Telegram-каналу в т.зв. «чорних» списках**

Державні інституції, які здійснюють забезпеченням безпеки України в інформаційній сфері постійно працюють над виявленням мереж поширення ворожої дезінформації, періодично публікуючи дані, в тому числі, і стосовно ворожих Telegram-каналів. Тож працюючи над дослідженням Telegram-каналу варто перевіряти його присутність у списках, на кшталт «Списку каналів поширення ворожої пропаганди», сформованого Центром протидії дезінформації.

2.3 / FACEBOOK

Для розпізнавання неавтентичної поведінки на сторінках профілів та спільнот у соцмережі Facebook, необхідно звертати увагу на залученість аудиторії, а також співвідношення вподобань і підписок. Водночас важливо звертати увагу на наповненість сторінки. Багато фейкових сторінок у Facebook не мають додаткової інформації, адже неавтентичні профілі не витрачають часу для створення правдоподібної сторінки.

Для перевірки сторінки у Facebook рекомендовано звертати увагу на наступне:

- **Інформація**

Напевно, найважливіший розділ для аналізу будь-якої сторінки в соцмережі. Ця частина має важливі відомості, які допоможуть у подальшому аналізі сторінки: контактні дані, опис сторінки або профілю, інші соцмережі, кількість підписок, кількість вподобань, відгуки на сторінку, посилання на інші веб-сайти та додаткова інформація про сторінку.

- **Розділи Фотографій та Відео**

Обидва зазначені розділи можуть надати додаткову інформацію в аналізі, адже деякі сторінки або спільноти дозволяють своїм користувачам публікувати фотографії. У такий спосіб аналітик може ретельно перевірити опубліковані світлини та знайти потрібні йому зв'язки для остаточного висновку.

- **Спільноти**

Іноді на публічних сторінках Facebook можна знайти розділ зі спільнотою. Цей розділ може надати додаткову інформацію про аналізовану мережу, а також розуміння, чи є на сторінці бот-активність. Наприклад, у спільноті з кількома десятками тисяч підписників, публікації отримують лише 100-200 реакцій. Вказане свідчить про бот-активність.

- **Інше**

На сторінках Facebook користувачі або адміністратори самі вирішують, які додаткові розділи матиме їхня сторінка. Тож, під час аналізу важливо ретельно переглядати інші розділи, які можуть містити інформацію про інтереси спільноти.

2.4 / YOUTUBE

Для аналізу неавтентичного контенту на відеохостингу YouTube та сторінок, що його публікують, сама платформа містить достатню кількість наявних даних: кількість коментарів, переглядів та підписників. Важливо враховувати, що активність ботів у коментарях можна визначити за текстом самих коментарів. Так, коментарі від ботів у більшості випадків не мають змісту або дуже прості за своїм характером.

У аналізі YouTube-каналу має значення перегляд інших розділів на ньому. У розділі «Про канал» знаходяться додаткові посилання каналу, регіон, дата створення, кількість загальних переглядів, контактні дані та опис. Також існують розділи «Спільнота» і «Канали», звідки аналітик може отримати додаткову інформацію.

Важливо зазначити, що з появою формату Youtube Shorts значна кількість фейкових відео подається саме через скорочений формат. Це зумовлено тим, що такі відео легше створювати на смартфоні, а завдяки короткому формату алгоритми YouTube швидше їх розповсюджує на ширшу аудиторію.

Для поглибленого аналізу YouTube-каналу існують різноманітні інструменти, але найдоступнішим у своєму використанні є
socialblade.com

Вказаний сайт дає можливість отримати детальну інформацію про досліджуваний канал. У більшості випадків для аналізу потрібен розділ «Детальна статистика». У цьому розділі є інформація про приріст переглядів та підписок каналу протягом певного проміжку часу. Ці дані дають можливість прослідкувати неорганічні прирости переглядів, а також неавтентичну активність на каналі.

2.5 / ВЕБ-САЙТИ

- **URL-посилання**

Під час інформаційних операцій ворог може створювати безліч фейкових ресурсів, які потрібно ретельно перевіряти. Спочатку важливо перевірити посилання на ресурс, адже ворог може створювати ресурси, які імітують оригінальні. Важливо зазначити, що потрібно звертати увагу на протокол посилання. Іноді фейкові медіаресурси використовують протокол http://, який є незахищеним. Річ у тому, що в такому випадку дані передаються у відкритому вигляді. Це створює ризик розкрити конфіденційну інформацію, у випадку, якщо хтось перехопить трафік. https:// вирішує цю проблему, додаючи в початковий протокол можливість шифрування даних. Також важливо звертати увагу на закінчення посилання, наприклад, оригінальний сайт «BBC» має посилання https://www.bbc.com/, фейкові у свою чергу можуть виглядати так– http://www.bbc.com.co/

- **Заголовок**

Головне завдання заголовка – створення інтересу з метою стимулювання користувач для переходу на сторінку ресурсу. Тому, надзвичайно важливо звертати увагу на те, які емоції заголовок може викликати.

- **Автор**

Зазвичай на фейкових медіаресурсах відсутній автор, що може слугувати показником неправдивості інформації. Якщо в сумнівній статті вказаний автор, то його важливо перевірити на предмет того, які ще статті ним було написано. Зазвичай, реальні автори статей активні в соцмережах, що дає можливість перевірити їх контент за межами сайту.

- **Джерела**

Джерела у статтях надзвичайно важливі, навіть коли публікації автентичні. Через них можна зрозуміти, звідки автор черпав інформацію і якими були його наміри.

Тому, важливо перевіряти усі зазначені джерела, а за їх відсутності робити правильні висновки.

- **Контент**

Під час прочитання тексту можна зробити логічний підсумок цілей та ідей, що закладені в статті. Потрібно розуміти та розрізняти інформативну або аргументативну статтю. В якому стилі вона написана, на яких засадах або фактах. Для цього важливо уважно прочитати статтю, при потребі навіть кілька разів, і виокремити її основні тези.

- **Зображення**

У текстах статті автор може використовувати зображення, які теж потрібно ретельно перевіряти. Автентичність зображень можна перевірити, використовуючи онлайн-ресурси, зазначені у розділі «2.1. X (Twitter)».

- **Коментарі та активність на сторінці публікації**

В основному медіаресурси містять окремий розділ з коментарями. Він також є важливим для аналізу, бо ворог може наповнювати його фейковими коментарями та переписками між користувачами, що надає статті більш правдоподібного вигляду. Важливо зазначити, що під час інформаційних операцій ворог може використовувати посилання на фейкові медіаресурси для того, щоб створити видимість популярності статті.

- **Інша інформація**

Під час аналізу медіаресурсів важливо звертати увагу на інші дані, що вказані наприкінці сторінки. Зазвичай компанії залишають потрібну інформацію для користувача, а саме: юридична адреса, посилання на соцмережі, юридичні контактні дані, поштова скринька, реєстрація та авторські права, політика конфіденційності та інше.

3/
ТОП-10 МЕХАНІЗМІВ ІНФОРМАЦІЙНОГО ВПЛИВУ РОСІЙСЬКОЇ ПРОПАГАНДИ

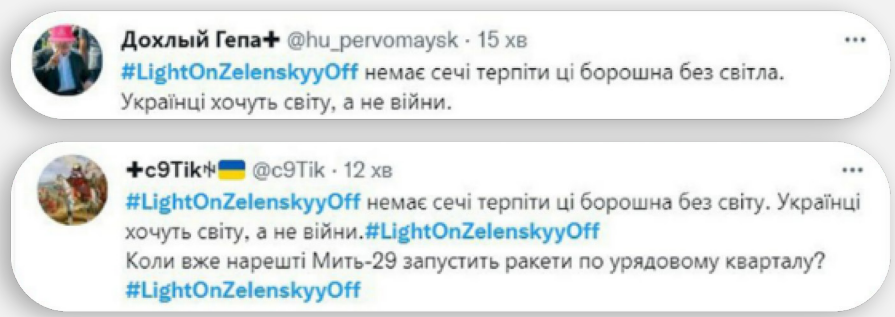
3.1 / БОТ

Спеціальна програма, що автоматично та/або за заданим алгоритмом виконує дії через ті ж самі інтерфейси, що і звичайний користувач, таким чином імітуючи його. Наприклад, мова може йти про пости у різних групах мережі Facebook, репости, ретвіти та коментарі у багатьох соцмережах, зокрема X, Telegram, TikTok, YouTube тощо.

У автоматичному режимі ботами може здійснюватися поширення попередньо підготовлених коментарів чи їх генерування за попередньо заданими параметрами. Ботоферма, тобто певна сукупність схожих або й однаковим чином запрограмованих ботів, може діяти як цілеспрямована та скоординована група акаунтів, що поширюють певний меседж, що відповідає ворожому наративу, та – кінцево – ворожим інтересам.
Боти можуть управлятися як в автоматичному режимі, і тоді вони множать коментарі, лайки або поширення. Утім, дуже часто через бот-акаунти у ручному режимі вороги генерують, видозмінюють та поширюють меседжі, які дуже складно відрізнити від меседжів реальної людини. Хіба що ця людина дійсно щиро є ворогом України, спілкується українською, утім, висловлює ідеї “русского міра”.

Іноді бот може прикидатися “корисним ідіотом”, тобто запевняти читачів у повній лояльності до України та української самобутності. І при цьому в наступному ж реченні – поширювати ворожі наративи.

Як це виглядає?



Як з цим боротися?

- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

3.2 / СОКПАПЕТ

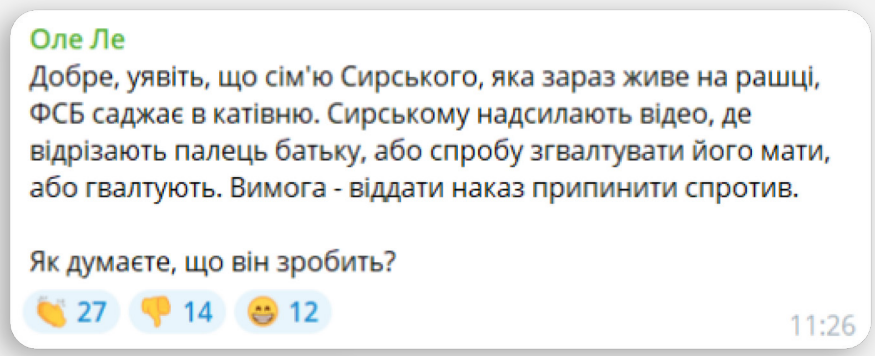
Це якраз і є той “бот-акаунт”, який не просто шерить інформацію, але й має ручне управління, тож варто розглянути його детальніше, адже такі акаунти можуть бути присутніми та активними в регіональному інформаційному просторі.

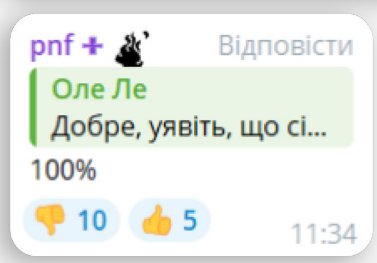
Сокпапет – це шахрайський обліковий запис, яким керує анонімна особа (наприклад, працівник ворожих спецслужб, або ж шахрай, що прагне виманити кошти у жертв), що приховує свої наміри. Такі фальшиві особистості використовуються для вступу в інтернет-спільноти з метою участі у обговореннях, нав’язування певних емоційних станів, маніпуляціях, дезінформації.

Умовна Наталія Іваненко з умовної групи “Суми благодійні”, яка пише розпачливі наративи про те, що все сумське кладовище за два роки розрослося в 3 рази, найчастіше виявляється ворожим сокпапетом. У кращому разі вона може бути “корисною ідіоткою”, яку переконав у правдивості історії про “сумське кладовище” ворожий сокпапет.

Іще одна постійно релевантна методика ворожої пропаганди – штучні діалоги кількох сокпапетів, які стимулюють дискусії, провокують негативні настрої, підтверджують “слова одне одного”. Наприклад, якщо до умовної Наталії Іваненко приєднується в бесіді умовна Viktoria Dets, чи умовний Владимир Моисеенко, і пише, що справді вони вчора ховали сина, і кладовище дійсно в 3 рази більше, ніж було до вторгнення, і це вже її третій син, який гине, і що влада хоче всіх убити, а не миритися з росією.... Ймовірно, ви маєте справу з нав’язуванням ворожих наративів працівником ворожої спецслужби з двох підконтрольних акаунтів.

Як це виглядає?





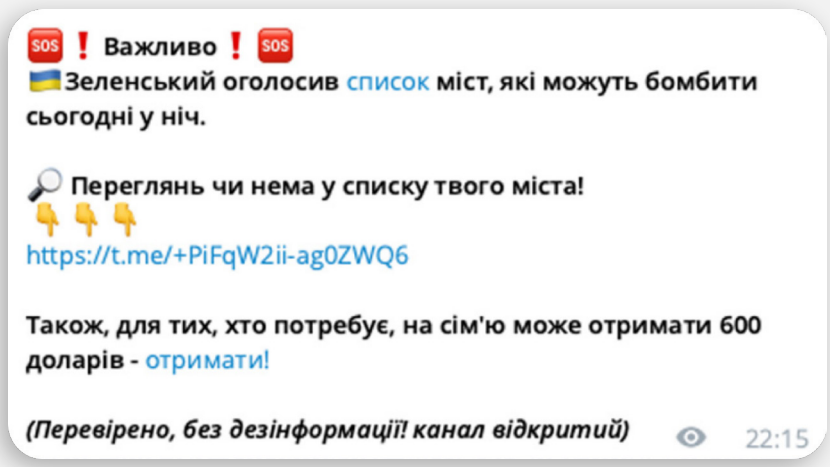
Як з цим боротися?

- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

3.3 / КЛІКБЕЙТ

Це універсальний маркетинговий механізм формування привабливої “упаковки” контенту. Його ключова мета – “клікабельність”, тобто такий підбір заголовку, ілюстрації, банерного зображення або відео, яке стимулює реципієнта натиснути на лінк на інформації (“читати далі” в Facebook, перейти на відео в YouTube тощо). Клікбейт – це нормальне явище в сучасному світі сенсаційних новин, гучних заголовків та зображень, що приваблюють увагу. На жаль, клікбейт як метод використовує і ворожа пропаганда. Відрізнити клікбейт ворогів можна за присутністю ворожих наративів у заголовку, текстовому блоці інформаційного повідомлення, або ж зображенні. Зазвичай “клікбейтні” повідомлення такого типу “обіцяють” глядачеві відповісти на “сенсаційні” питання, або ж передбачити завершення війни, можливі атаки на українські території абощо. А після натискання є ризик або потрапити на ворожу пропаганду, або навіть втрапити до рук шахраїв.

Як це виглядає?



Як з цим боротися?

- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

3.4 / РЕЙТИНГУВАННЯ

Соціологічні опитування – це складний регламентований механізм дослідження громадської думки, що потребує верифікації даних. Простіше кажучи, проводити такі опитування мають право чимало організацій, як в Україні так і на росії, утім, на жаль, нерідко результатами таких опитувань можна маніпулювати. Хоча якщо говорити про російську "соціологію", то в тоталітарній державі їй вірити точно не можна.

Навіщо ж маніпулюють цією інформацією? Мета – легітимізувати, тобто переконати спільноту в достовірності певних даних. "Рейтингування" – це механізм маніпулятивного, або навіть фальсифікуючого впливу на громадську думку, який прикривається формою "соціологічного опитування", за результатами якого складаються певні "рейтинги" або ж інші висновки та результати, які свідчать на користь замовників, тобто агентів впливу.

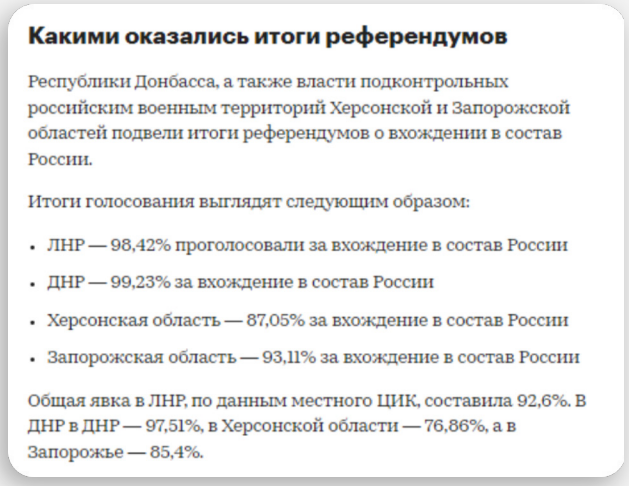
рф нерідко через фальсифікацію або спотворення соціологічних досліджень, і зокрема опитувань, може транслювати вигідні наративи. Наприклад, можуть використовуватися сфальсифіковані опитування на тимчасово окупованих територіях, для того, аби хтось із жертв такої дезінформації, не виявивши критичного мислення, повірив у них. Наслідком може бути або недовіра до української, зокрема регіональної влади, панічні настрої, омана щодо підтримки в Україні "русского міра" тощо.

Саме тому будь-яке розповсюдження соціологічної інформації, що не має достовірного посилання – на авторитетну соціологічну організацію, на кінцевий файл із подробицями опитування тощо, однак – збігається з наративами ворога, потребує додаткової перевірки Якщо ви контролюєте ресурс, де може з'явитися така інформація, або ж уже опублікована – необхідно або видалити та спростувати дані, опубліковані раніше, або ж відмовитися від публікації.

Як це виглядає?

Окончательные результаты референдума в Крыму: 96,77% участников или 1 млн 233 тыс. 2 крымчанина хотят в Россию

В Симферополе подведены окончательные результаты референдума в Крыму. По итоговым данным, за воссоединение с Россией проголосовали 96,77% принявших участие в голосовании жителей Крыма.



Какими оказались итоги референдумов

Республики Донбасса, а также власти подконтрольных российским военным территорий Херсонской и Запорожской областей подвели итоги референдумов о вхождении в состав России.

Итоги голосования выглядят следующим образом:

- ЛНР — 98,42% проголосовали за вхождение в состав России
- ДНР — 99,23% за вхождение в состав России
- Херсонская область — 87,05% за вхождение в состав России
- Запорожская область — 93,11% за вхождение в состав России

Общая явка в ЛНР, по данным местного ЦИК, составила 92,6%. В ДНР в ДНР — 97,51%, в Херсонской области — 76,86%, а в Запорожье — 85,4%.

Як з цим боротися?

- Встановити джерело проведення соціологічного опитування з метою визначення рівня його авторитетності.
- Віднайти дослідження, результати якого публікуються в медіа, з метою визначення його загального контексту.
- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

3.5 / АНОНІМНИЙ АВТОРИТЕТ

Ворожа пропаганда нерідко використовує дуже прості, однак неочевидні для нефахівців прийоми спрямованого психологічного впливу. Одним із них є надання певним тезам в рамках наративу легітимності (достовірності, переконливості) за рахунок посилання на достовірне на вигляд джерело, яке при цьому має певний експертний статус. Такий статус може натякати на “джерело таємниці”, тобто недоступної загалу інформації. Або ж на особливий зв’язок “автора” повідомлення та “джерела”, яке транслює таку “таємницю”.

Простіше кажучи, ботоводи за рахунок ботів або сокпапетів розповсюджують тези про те, що “їхнє” близьке джерело (родич або близький товариш із доступом до закритої інформації) розповів “по секрету” певну таємну інформацію. Цей родич, друг абощо точно “знає” про щось (ракетний удар, наступ з Півночі, секретні переговори, або ж підставте знайомий вам варіант). Якщо такі судження висловлюють в закритих спільнотах, або ж в групах, особливо – регіонального, громадського рівня – авторитетність таких повідомлень в очах емоційно нестабільних людей, які не володіють навичками критичного мислення, може виглядати безпідставно високою.

Іншими словами, налякати або переконати в сусідському чаті або Facebook-групі людей якоюсь “сенсацією”, поданою за принципом анонімного авторитета – це вплив на людей. Теми можуть бути найрізноманітнішими – від дій ворога, бездіяльності або “неправильної” діяльності українських сил, і аж до “свавілля ТЦК”, коли “мій сват, який працює в ТЦК, каже, що у них по місту їздить 4 бригади на швидких і пакує чоловіків у темних дворах”. Тож повідомлення, які транслюють наративи ворога в подібний спосіб, необхідно виявляти, а також пояснювати ширшим колам людей, як їх виявити та чому не варто їх сприймати всерйоз.

Як це виглядає?

Як з цим боротися?

- Встановити достовірність описаного в дописі (події, документа тощо).
- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

3.6/ ДІПФЕЙК

Технології штучного інтелекту нині дозволяють настільки глибоку та ґрунтовну обробку зображення та звуку, що отримані в результаті такої роботи відео-файли можуть бути дуже схожими на реально зняті на камеру, тобто документальні. Діпфейки – це приклади таких непомітно на перший погляд змінених фото, або ж останніми роками особливо популярними стають відео-діпфейки.

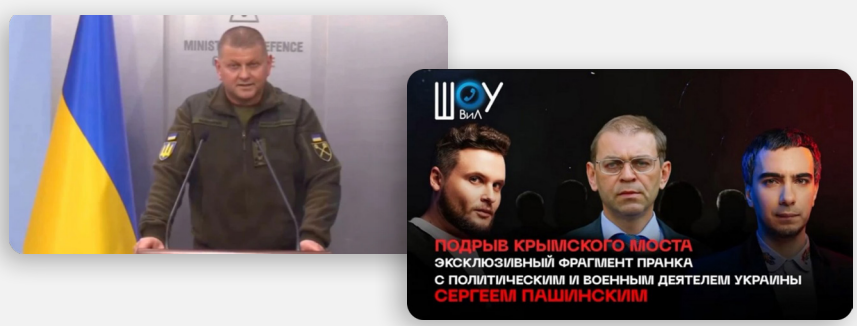
Часто це безневинні розважальні відео, які може запрограмувати в спеціальних додатках навіть школяр. Дональд Трапм може привітати вам із Днем народження, правдоподібно “розтуляючи рота” під слова, які ви пропонуєте використати додатку. Папа Римський “може” лихословити, відомі актори — зізнаватися в злочинах і так далі. Діпфейки, зрештою, активно використовуються не лише заради розваги, а й заради політичних маніпуляцій громадською думкою. На жаль, наш ворог також вдається до цього ганебного фальсифікаторського механізму.

Регіональним лідерам особливо важливо берегтися від спрямованого впливу, адже діпфейки можуть використовуватися і як “маски” для онлайн-конференцій, і так ворог може претендувати на отримання чутливої або секретної інформації. Тому до онлайн-зустрічей з високим рівнем відповідальності варто готуватися, враховуючи момент перевірки співрозмовника на використання технології діпфейку.

Утім, за допомогою діпфейків не лише можуть вивідати секрети, але й змусити людей повірити у певні тези. Так, доволі ілюстративним прикладом у цьому випадку може слугувати серія з трьох діпфейків, направлених на дискредитацію Валерія Залужного. У першому діпфейку колишній Головнокомандувач Збройних Сил України повідомляє про смерть свого помічника внаслідок вибуху та просить не дарувати йому подарунків. Після цього у мережі з’явилося інше відео, де В.Залужний нібито розповідає, що Зеленський намагається його ліквідувати та здати країну росії. В третьому записі він вже спростовує інформацію, що всі минулі записи – це фейк, і наказує військовим захоплювати владу.

Але якщо говорити про віртуальну реальність, на жаль, діпфейки здатні переконати довірливих людей у негативній щодо інтересів України інформації, на кшталт “капітуляції України”, “здачі міст” та подібного. Мета – дезінформувати, посіяти паніку. Саме тому виявляти та робити дії для обмеження поширення таких діпфейків – це суттєва допомога регіональних лідерів думок, якій вони можуть ефективно сприяти в інформаційній сфері на регіональному рівні.

Як це виглядає?



Як з цим боротися?

- Дуже ретельно перевіряти осіб, з якими організовуються онлайн зустрічі.
- У ході онлайн спілкування необхідно придивлятися на неприродні рухи очей, а також звертати увагу на невідповідність кольорів та освітлення.
- У реальному часі діпфейк можна розпізнати, якщо особа поверне свою голову. Це означає, що пряма трансляція діпфейку не може зі 100% вірогідністю обробляти інші частини обличчя.

3.7 / КОНТЕКСТОМІЯ

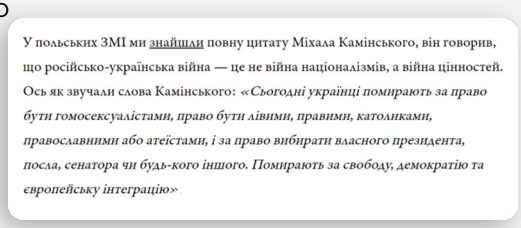
Маніпуляції можуть нині проводитися не лише із візуальною чи аудіо-інформацією, але й із текстами. Особливо – якщо йдеться про відповідальні заяви офіційних осіб, які складно сфальсифікувати повністю. Утім, зробивши з текстом кілька малопомітних маніпуляцій, зловмисними можуть отримати та розповсюдити вигідний для них наратив.

Контекстомія – такий механізм інформаційного впливу, суть якого полягає у вилученні уривку тексту з навколишнього матеріалу таким чином, щоб спотворити його задумане автором значення. Контекстомії можуть бути як навмисними, так і випадковими, якщо хтось неправильно розуміє сенс і пропускає щось суттєве для його прояснення, вважаючи його несуттєвим.

Особливо небезпечна така маніпуляція з офіційними заявами. Приміром, вилучене із заяви речення, риторичне питання, чи бодай одне слово, може суттєво змінити сенс та, наприклад, посіяти паніку, або ж впринути на певні рішення відповідальних осіб. Саме тому варто отримувати інформацію для прийняття рішень лише з офіційних джерел, які відзначаються високою мірою достовірності та доводили її роками, та неодмінно перевіряти цю інформацію в додаткових джерелах. Особливо це стосується регіональних редакцій, які працюють з потенційно впливовою інформацією, що може дати стимул певній поведінці в регіоні.

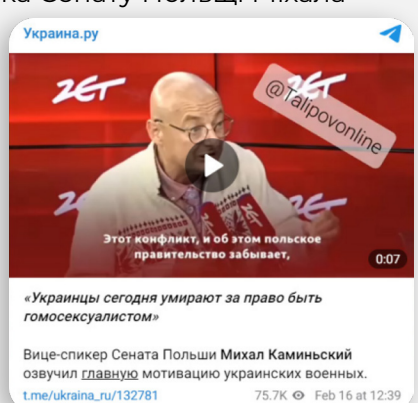
Як це виглядає?

Оригінал цитати віцемаршалека Сенату Польщі Міхала Камінського



У польських ЗМІ ми знайшли повну цитату Міхала Камінського, він говорив, що російсько-українська війна — це не війна націоналізмів, а війна цінностей. Ось як звучали слова Камінського: *«Сьогодні українці помирають за право бути гомосексуалістами, право бути лівими, правими, католиками, православними або атеїстами, і за право вибирати власного президента, посла, сенатора чи будь-кого іншого. Помирають за свободу, демократію та європейську інтеграцію»*

Уривок, вилучений з цитати віцемаршалека Сенату Польщі Міхала Камінського



Як з цим боротися?

- Віднайти першоджерело цитованого тексту чи прямої мови автора цитати.
- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

3.8 / ІНФОРМАЦІЙНЕ АЛІБІ

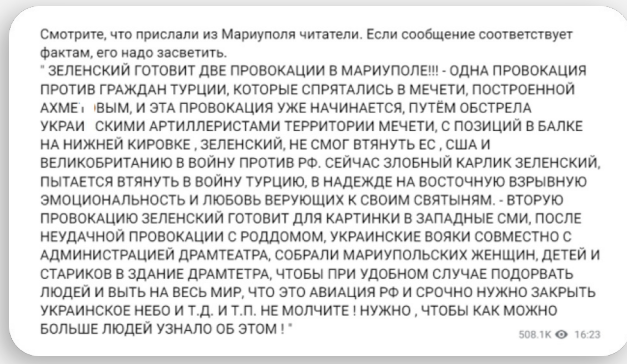
Цей жорстокий механізм інформаційного впливу росія використовує в найкривавіших злочинанах. Його суть полягає у превентивному звинуваченні однією стороною іншої в діях, які були чи лише будуть вчинені нею ж, першою стороною. Наприклад, росія звинувачує українську сторону в плануванні обстрілів мирного населення в регіоні, який пізніше буде обстріляно артилерією рф.

Інформаційне алібі може використовуватися і як залякування іншої сторони, або ж міжнародної спільноти, кривавими та серйозними діями, підготовка до яких нібито йде. Тоді заяви сторони, наприклад росії, про те, що нібито готується якась серйозна деструктивна діяльність з боку України, можуть сприйматися як погрози вчинити такі дії. Саме тому треба дуже уважно слідкувати за тим, як трактує українське керівництво ті або інші заяви російської федерації. У більшості випадків приклади використання механізму “інформаційного алібі” може виявитися блефом. Але завжди треба уважно досліджувати такі питання.

Як це виглядає?

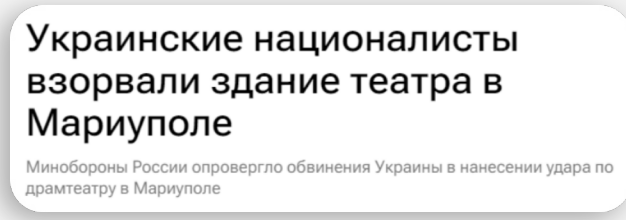
Етап перший: «Інформаційна закладка»

12.03.2022 року. Російський TG-канал «Русский тарантасъ» анонсував знищення Маріупольського драмтеатру, яке нібито готується українською стороною.


Смотрите, что прислали из Мариуполя читатели. Если сообщение соответствует фактам, его надо засветить.
" ЗЕЛЕНСКИЙ ГОТОВИТ ДВЕ ПРОВОКАЦИИ В МАРИУПОЛЕ!!! - ОДНА ПРОВОКАЦИЯ ПРОТИВ ГРАЖДАН ТУРЦИИ, КОТОРЫЕ СПРЯТАЛИСЬ В МЕЧЕТИ, ПОСТРОЕННОЙ АХМЕ ВЫМ, И ЭТА ПРОВОКАЦИЯ УЖЕ НАЧИНАЕТСЯ, ПУТЁМ ОБСТРЕЛА УКРАИ СКИМИ АРТИЛЛЕРИСТАМИ ТЕРРИТОРИИ МЕЧЕТИ, С ПОЗИЦИЙ В БАЛКЕ НА НИЖНЕЙ КИРОВКЕ , ЗЕЛЕНСКИЙ, НЕ СМОГ ВТЯНУТЬ ЕС , США И ВЕЛИКОБРИТАНИЮ В ВОЙНУ ПРОТИВ РФ. СЕЙЧАС ЗЛОБНЫЙ КАРЛИК ЗЕЛЕНСКИЙ, ПЫТАЕТСЯ ВТЯНУТЬ В ВОЙНУ ТУРЦИЮ, В НАДЕЖДЕ НА ВОСТОЧНУЮ ВЗРЫВНУЮ ЭМОЦИОНАЛЬНОСТЬ И ЛЮБОВЬ ВЕРУЮЩИХ К СВОИМ СВЯТЫНЯМ. - ВТОРУЮ ПРОВОКАЦИЮ ЗЕЛЕНСКИЙ ГОТОВИТ ДЛЯ КАРТИНКИ В ЗАПАДНЫЕ СМИ, ПОСЛЕ НЕУДАЧНОЙ ПРОВОКАЦИИ С РОДДОМОМ, УКРАИНСКИЕ ВОЯКИ СОВМЕСТНО С АДМИНИСТРАЦИЕЙ ДРАМТЕАТРА, СОБРАЛИ МАРИУПОЛЬСКИХ ЖЕНЩИН, ДЕТЕЙ И СТАРИКОВ В ЗДАНИЕ ДРАМТЕТРА, ЧТОБЫ ПРИ УДОБНОМ СЛУЧАЕ ПОДОРВАТЬ ЛЮДЕЙ И ВЫТЬ НА ВЕСЬ МИР, ЧТО ЭТО АВИАЦИЯ РФ И СРОЧНО НУЖНО ЗАКРЫТЬ УКРАИНСКОЕ НЕБО И Т.Д. И Т.П. НЕ МОЛЧИТЕ ! НУЖНО , ЧТОБЫ КАК МОЖНО БОЛЬШЕ ЛЮДЕЙ УЗНАЛО ОБ ЭТОМ ! "
508.1K 16:23

Етап другий: «Безапеляційне звинувачення»

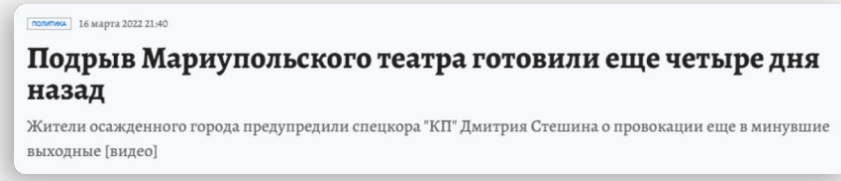
16.03.2022 року. Після знищення Маріупольського драмтеатру російськими війська, російська сторона розпочала медійну кампанію, метою якої стало безапеляційне звинувачення України у вчиненні цього злочину.


Украинские националисты взорвали здание театра в Мариуполе

Минобороны России опровергло обвинения Украины в нанесении удара по драмтеатру в Мариуполе

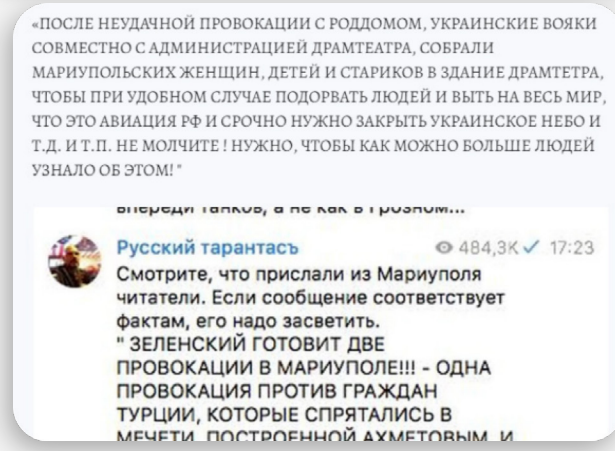
Етап третій: «Відсилка до інформаційної закладки»

16.03.2022 року. Одразу після удару російських військ по Маріупольському драмтеатру, в російському медіапросторі розпочалося поширення публікації TG-каналу «Русский тарантасъ» від 12.03.2022 року з анонсом знищення Маріупольського драмтеатру, яке нібито заздалегідь готувалося українською стороною. Така відсилка до «інформаційної закладки» мала на меті переконання аудиторії у тому, що згаданий злочин нібито вчинила українська сторона.


ПОЛИТИКА 16 марта 2022 21:40

Подрыв Мариупольского театра готовили еще четыре дня назад

Жители осажденного города предупредили спецкора "КП" Дмитрия Стешина о провокации еще в минувшие выходные [видео]


«ПОСЛЕ НЕУДАЧНОЙ ПРОВОКАЦИИ С РОДДОМОМ, УКРАИНСКИЕ ВОЯКИ СОВМЕСТНО С АДМИНИСТРАЦИЕЙ ДРАМТЕАТРА, СОБРАЛИ МАРИУПОЛЬСКИХ ЖЕНЩИН, ДЕТЕЙ И СТАРИКОВ В ЗДАНИЕ ДРАМТЕТРА, ЧТОБЫ ПРИ УДОБНОМ СЛУЧАЕ ПОДОРВАТЬ ЛЮДЕЙ И ВЫТЬ НА ВЕСЬ МИР, ЧТО ЭТО АВИАЦИЯ РФ И СРОЧНО НУЖНО ЗАКРЫТЬ УКРАИНСКОЕ НЕБО И Т.Д. И Т.П. НЕ МОЛЧИТЕ ! НУЖНО, ЧТОБЫ КАК МОЖНО БОЛЬШЕ ЛЮДЕЙ УЗНАЛО ОБ ЭТОМ! "

Русский тарантасъ 484,3K 17:23
Смотрите, что прислали из Мариуполя читатели. Если сообщение соответствует фактам, его надо засветить.
" ЗЕЛЕНСКИЙ ГОТОВИТ ДВЕ ПРОВОКАЦИИ В МАРИУПОЛЕ!!! - ОДНА ПРОВОКАЦИЯ ПРОТИВ ГРАЖДАН ТУРЦИИ, КОТОРЫЕ СПРЯТАЛИСЬ В МЕЧЕТИ, ПОСТРОЕННОЙ АХМЕТОВЫМ, И

Як з цим боротися?

- Визначити рівень небезпечності потенційної загрози та наслідків, що можуть настати.
- При високому рівні небезпечності потенційної загрози чи великій імовірності настання прогнозованих негативних наслідків, рекомендується розпочинати комунікацію «на випередження».
- Комунікація повинна бути побудована з урахуванням можливого провокування панічних настроїв серед населення.

3.9 / «ТРУДНОЩІ ПЕРЕКЛАДУ»

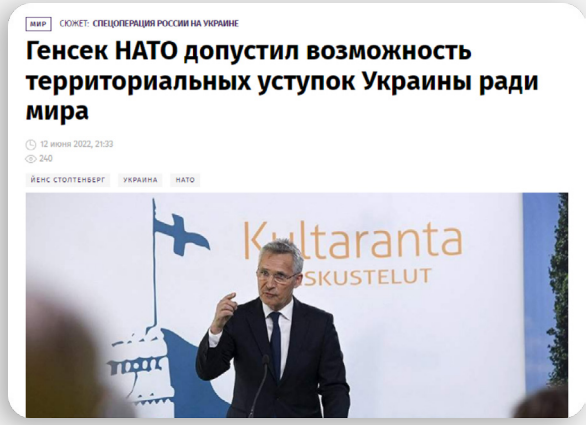
Іще один механізм інформаційного впливу, пов'язаний із міжнародним контекстом. Наші вороги схильні значно применшувати значимість невигідної для себе інформації та перебільшувати – вигідної. При цьому часто "невигідну" інформацію перетворюють на "вигідну" шляхом банальних маніпуляцій із перекладом. Приміром, якісь терміни можуть перекласти у вигідніший для себе бік, або навіть простіше – вільно поставити кому або крапку в переказі усного мовлення – і це вже може вплинути на сприйняття.

Завдяки таким маніпуляціям, навіть найавторитетніші "болгарські політики" можуть "захоплюватися" якимись фразами путіна тільки тому, що вислови болгарською можуть "вільно перекласти", а перевіряти з читачів ніхто не буде, риючись у болгарських ЗМІ. Утім, цей приклад – з російського контексту.

На жаль, деякі окремі українські ЗМІ, а в більшій мірі – блогери та лідери думок у соціальних мережах – можуть використовувати російські медійні "помийки" як джерела альтернативної інформації. І звідти можуть просочуватися "труднощі перекладу" якогось міжнародного контексту щодо російсько-української війни, спотворені російською пропагандою. Через цитати таких "сернсацій", а також через спрямовані дії ворогів за рахунок поширення такої інформації через ботів, вони можуть досягати заданого психологічного ефекту.

Як це виглядає?

Прилад реалізації механізму “труднощі перекладу”



Оригінал цитати Генерального секретаря НАТО Єнса Столтенберга

«Тож чи можливий мир — це не питання. Питання, яку ціну ви готові заплатити за мир. Скільки території? Скільки незалежності? Скільки суверенітету? Скільки свободи? Скільки демократії готові пожертвувати заради миру? І це дуже складна моральна дилема. І судити про це мають ті, хто платить найвищу ціну. Наш обов'язок – підтримувати їх». («So that was 'peace is possible' – that's not the question anyway, the question is: what price are you willing to pay for peace? How much territory? How much independence? How much sovereignty? How much freedom? How much democracy are you willing to sacrifice for peace? And that's a very difficult moral dilemma. And it's for those who are paying the highest price to make that judgement. Our responsibility is to support them.)»

Як з цим боротися?

- Віднайти першоджерело цитованого тексту чи прямої мови автора цитати.
- Зробити максимально точний (дослівний) переклад віднайденого тексту.
- Провести оцінку рівня небезпечності наслідків, що можуть настати.
- При високому рівні небезпечності прогнозованих негативних наслідків, рекомендується розпочинати комунікацію.

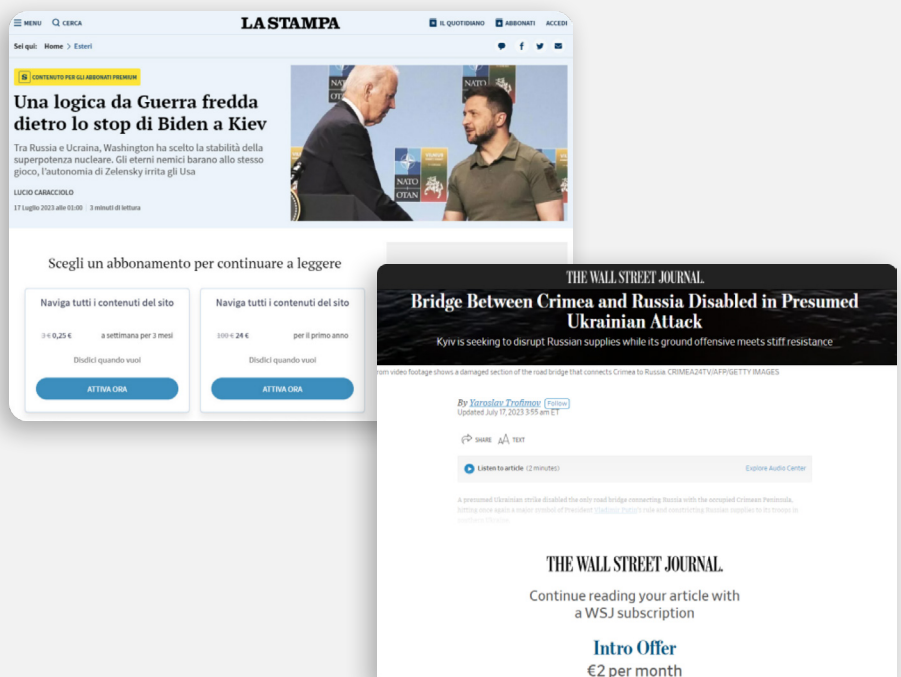
3.10 / «ПЕРЕВІР, ЯКЩО ЗМОЖЕШ»

Вороги нерідко використовують цей механізм, коли намагаються добитися ефекту враження щодо негативного ставлення або недовіри до майбутнього України в міжнародному контексті. Іншими словами, росія може просувати свої наративи, спрямовані на зневіру наших громадян в перемозі України, конспіруючи їх під цитати з авторитетних міжнародних джерел, які неможливо перевірити, адже для доступу потрібно мати підписку.

Це – іще одне свідчення того, що довіряти російським та афільованим з їхніми інтересами ЗМІ – точно не варто. У жодному разі не варто не те що не посилатися на такі джерела інформації, але й сприймати їх усерйоз, а тим паче приймати на основі такої інформації певні рішення.

Інформацію з міжнародного контексту завжди варто перевіряти за допомогою дослідження цієї теми в українських ЗМІ, а передовсім – у офіційних заявах. Якщо ж є необхідність з'ясувати правдивіть такої інформації, і водночас – немає доступу до першоджерела – завжди можна послати запит у компетентні структури, і отримати достовірну інформацію.

Як це виглядає?



Як з цим боротися?

- Створити підбірку іноземних медіа, які найбільш часто цитують та/або посилаються на того чи іншого спікера або державний орган.
- У разі використання ворожою стороною механізму "перевір, якщо зможеш" – звертатися до Центру протидії дезінформації чи українських фактчекінгових проєктів, таких як VoxCheck.
- За наявності відновідного фінансування, забезпечити підписку на попередньо визначені іноземні медіа для можливості здійснення перевірити достовірність цитованого тексту.

4 / ФАКТЧЕКІНГ

Як у регіональних ЗМІ, так і в органах регіональної влади можуть з'явитися потреби у самостійному здійсненні фактчекінгу. Загалом фактчекінг – тобто перевірка певної інформації на достовірність – є важливою навичкою журналістів та усіх осіб, які працюють з важливою інформацією, і цією навичкою не варто нехтувати. А для того, щоби ви мали уявлення про ключові процеси та механізми, пов'язані з фактчекінгом, а також знали, як поглиблювати свої знання та розвивати навички на практиці, надаємо в цьому розділі ключові поради щодо фактчекінгу.

4.1 / ЯК ПЕРЕВІРЯТИ ФОТО ТА ВІДЕО

- **Зворотний пошук**

Головний інструмент для перевірки фото та відео — зворотний пошук зображень. Це можна зробити за допомогою інструментів Google Lens, PimEyes, TinEye, Bing. Також можна використовувати Yandex, особливо якщо треба знайти інформацію у російськомовному сегменті. Часто завдяки такому пошуку вдається знайти першоджерело або принаймні підказки, де продовжити перевірку. Також у браузері можна встановити плагін Fake News Debunker із кількома функціями: зворотний пошук зображень, аналіз метаданих, аналіз змін, зроблених на фото.

- **Інструменти, які допомагають проаналі-зувати зміни в зображеннях**

Forensically — сервіс для перевірки зображень. Дозволяє наближувати елементи фото, щоб виявити зміни (розділ Magnifier), виявити схожі елементи (розділ Clone Detection), проаналізувати змінені фрагменти на зображенні (розділи ELA та Noise Analysis).

FotoForensics – ще один інструмент для перевірки зображень. У різних розділах можна переглянути змінені фрагменти на зображенні (розділ ELA, як і у Forensically) або приховані пікселі (розділ Hidden Pixels).

Зважайте на те, що інструменти з аналізу зображень не працюють ідеально та почасти можуть видавати неправдиві результати. Відтак важливо не покладатися лише на них, а займатися так званим “даблчекінгом” – тобто багаторівневою, як мінімум подвійною перевіркою інформації.

- **Метадані**

Перевірити час та місце створення світлин допоможуть метадані, які містяться у зображеннях. Їх можна відкрити правим кліком миші на зображення в операційних системах Windows та Apple, і за допомогою кодування в Linux. Водночас можна скористатися онлайн сервісами, які дозволяють отримати доступ до прихованих метаданих ваших файлів: metadata2go.com

Приклад фактчеку

У Бразилії в рамках акції на підтримку України на статую Христа-Спасителя одягнули гігантську вишиванку:

Звучить малоймовірно. Інструменти з аналізу зображення у цьому випадку не показали, що світлину відредаговано, однак за зворотним пошуком зображення у Google ви можете знайти оригінальне фото, використане у фейку:

На те, що це оригінальне зображення, вказує однакове розміщення людей внизу світлини та однаковий ракурс.

4.2 / ЯК ВИЯВИТИ ПІДРОБЛЕНІ ДОКУМЕНТИ

Фейкороби часто фальсифікують документи – офіційні листи від адміністрації навчальних закладів, укази та розпорядження від державних органів, повістки, звіти, договори тощо. Тобто ця проблема може напряму стосуватися як відповідальності регіональних лідерів, так і поведінки з інформацією в регіональних ЗМІ. Виявити підробку можна за допомогою кількох способів:

- ***Помилки у тексті та оформленні***

Російські фейкороби часто припускаються помилок у перекладі, граматиці або пунктуації — це типові помилки, які ви навряд зустрінете у справжніх документах. Також зважайте на оформлення документа та порівняйте його з іншими від таких самих установ, аби перевірити, чи є між ними відмінності.

- ***Першоджерело***

За зворотним пошуком, описаним вище, або за ключовими словами у пошуковій системі, до прикладу в Google, знайдіть першоджерело документа. Якщо його не публікували органи, які буцімто й видали документ, навряд чи він автентичний. Щобільше, якщо першоджерелом документа є російський пропагандистський ресурс або анонімний користувач, у більшості випадків ви маєте справу з фейком.

- ***Імена, підписи та дати***

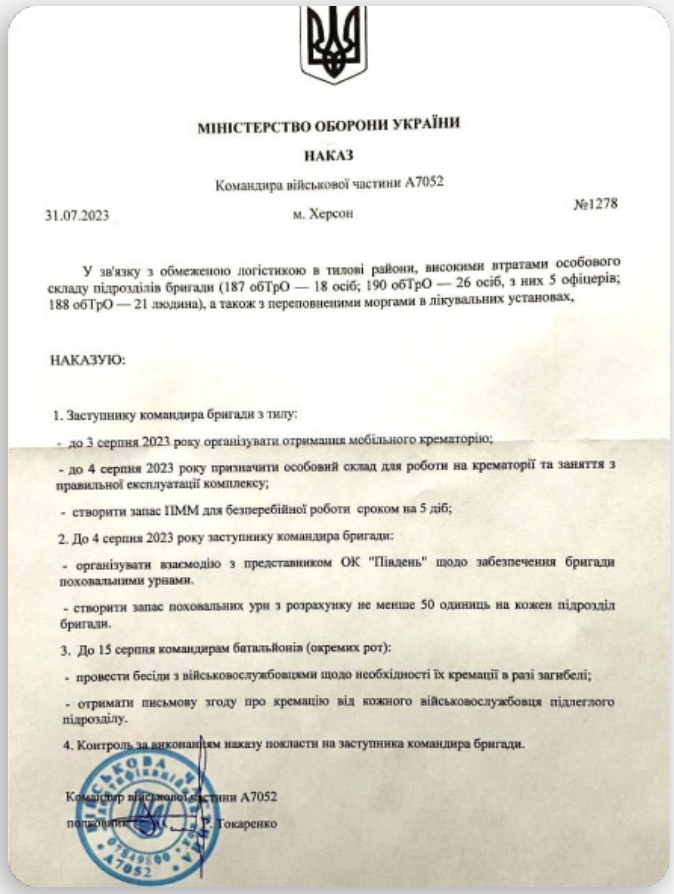
Перевірте, чи збігається посада людини, яка підписала документ, з інституцією, яка цей документ нібито видала. Якщо у відкритому доступі можна знайти підпис вказаної особи, порівняйте обидва підписи. Також фейкороби можуть помилитися з датою, до прикладу, вказати неправильний рік або неправильну назву установи — на це також варто звертати увагу.

- ***Номер документа***

Зазвичай в офіційних документах вказують номер, за яким ви зможете знайти ідентичний документ в онлайн-форматі на сайті відомства, яке його видало. Якщо за вказаним номером відображається інший документ або документа з таким номером взагалі не існує, ви маєте справу з підробкою.

Приклад фактчеку

Командир 123-ї бригади ТрО віддав наказ про створення мобільних крематоріїв, про що свідчить опублікований документ:



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

НАКАЗ

Командира військової частини А7052

31.07.2023 м. Херсон №1278

У зв'язку з обмеженою логістикою в тилові райони, високими втратами особового складу підрозділів бригади (187 обТрО — 18 осіб; 190 обТрО — 26 осіб, з них 5 офіцерів; 188 обТрО — 21 людина), а також з переповненими моргами в лікувальних установах,

НАКАЗУЮ:

1. Заступнику командира бригади з тилу:

- до 3 серпня 2023 року організувати отримання мобільного крематорію;

- до 4 серпня 2023 року призначити особовий склад для роботи на крематорії та заняття з правильної експлуатації комплексу;

- створити запас ПММ для безперебійної роботи сроком на 5 діб;

2. До 4 серпня 2023 року заступнику командира бригади:

- організувати взаємодію з представником ОК "Південь" щодо забезпечення бригади поховальними урнами.

- створити запас поховальних урн з розрахунку не менше 50 одиниць на кожен підрозділ бригади.

3. До 15 серпня командирам батальйонів (окремих рот):

- провести бесіди з військовослужбовцями щодо необхідності їх кремації в разі загибелі;

- отримати письмову згоду про кремацію від кожного військовослужбовця підлеглого підрозділу.

4. Контроль за виконанням наказу покласти на заступника командира бригади.

Командир військової частини А7052

полковник Р. Токаренко

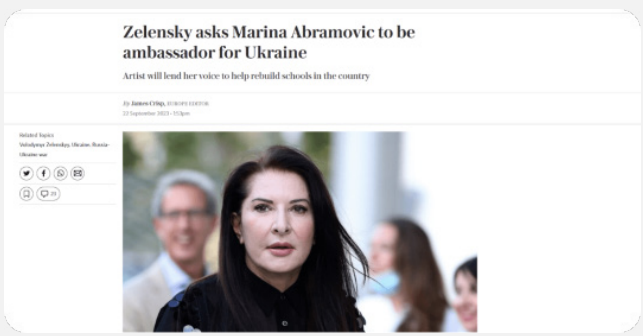
Однак документ містить помилки: у тексті вказано «сроком на 5 діб», коли правильно буде «строком на 5 діб». Також ім'я командира вказано неправильно — відповідно до останніх вимог оформлення офіційної документації, правильно було б написати не «Р. Токаренко», а «Роман ТОКАРЕНКО». Також варто звернути увагу на печатку військової частини. Код ЄДРПОУ «07849800», який на ній вказаний, не належить даній військовій частині. Організації з таким кодом не існує. Згодом 123-тя бригада ТрО на своїй офіційній фейсбук-сторінці заявила, що даний документ є черговим фейком російської пропаганди.

4.3 / ПОПЕРЕДНІ ВЕРСІЇ ВЕБСТОРІНКИ

Ви можете відслідкувати зміни у контенті сайтів за допомогою Internet Archive Wayback Machine – сервісу, який архівує попередні версії вебсторінок. Також у цьому допоможе кеш пошукових систем, доступний у Google, Bing та інших пошукових системах. Це надзвичайно корисні інструменти у випадках, коли потрібну вам інформацію змінили або видалили з вебсайту.

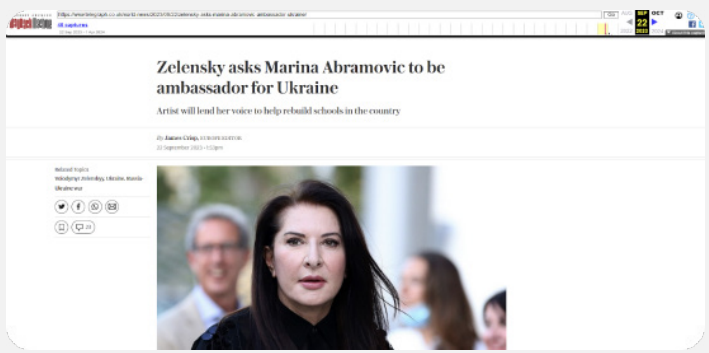
Приклад фактчеку

Володимир Зеленський запросив художницю Марину Абрамович стати посолкою України – про це повідомляють у виданні The Telegraph:



За заголовком статті, показаної на скриншоті, ви можете знайти публікації, що містять посилання на статтю The Telegraph з таким же заголовком. Сторінка більше недоступна, однак у вебархіві можна переглянути попередні версії сайту.

В одній із них ми бачимо статтю Джеймса Кріспа– автора, якого на скриншоті згадують російські ЗМІ.



За даними вебархіву, статтю дійсно публікували на сайті, однак, зрозумівши помилковість інформації, **видання видалило її через 2 дні після розміщення.**

4.4 / ЯК ПЕРЕВІРИТИ ЕКСПЕРТА

Перш ніж довіряти інформації, яку дає той чи інший експерт, варто з'ясувати:

1. яку він має освіту, чи компетентний він у питаннях, щодо яких висловлюється, адже якщо у "експерта" історична освіта, а він коментує теми вакцинації від ковіду, довіряти його думці не варто;
2. який він має досвід роботи, чи достатньо у нього професійних знань і досвіду, аби називати себе експертом із даного питання, наприклад, якщо тему вакцинації від ковіду коментує лікар, але його спеціалізація стоматологія, то його думці не варто довіряти;
3. його попередню риторику та виступи, наскільки послідовно він дотримувався тієї чи іншої думки, і якщо експерт кілька разів змінював свою думку і не пояснював це, то це означає, що його позиція може бути заангажованою;
4. думку щодо нього від експертів у цій сфері, тобто, чи довіряють його позиції, чи дослуховуються до нього "колеги по цеху", як коментують його виступи та його позицію.

Не варто зважати на велику кількість підписників у експерта, адже це не є показником об'єктивності. Також велика медійність та відомість експерта не є показником його обізнаності в тій чи іншій темі.

Для прикладу варто згадати Ларрі Джонсона, який наприкінці 80-их років кілька років працював аналітиком у ЦРУ, після чого перейшов до антитерористичного управління Державного департаменту США. У 1993 році Джонсон залишив державну роботу, щоб приєднатися до приватного сектору, «продовжуючи будувати подвійну кар'єру бізнес-консультанта та експерта з питань розвідки». Наразі цей колишній аналітик ЦРУ активно просуває кремлівські наративи на Заході, а проросійські ЗМІ, посилаючись на нього, розповідають своєму населенню, що думає про російську-українську війну справжній американський екс-аналітик ЦРУ.

4.5 / ЯК ПОВОДИТИСЯ У СОЦМЕРЕЖАХ (ТЕЛЕГРАМ, ФЕЙСБУК, ЮТУБ, ТВІТТЕР)

Соціальні мережі сьогодні є дуже потужними джерелами інформації. Саме тому необхідно мати базові навички поводження з ними, аби не натрапити на маніпулятивний контент, якого, на жаль, у соцмережах доволі багато. У попередніх розділах ми неодноразово торкалися специфіки окремих соцмереж та прикладів пропагандистських, інформаційно-психологічних та інших дій і акцій ворога, які поширювалися саме через соціальні мережі. Нижче ми тезово підсумуємо загальні позиції щодо поведінки в соцмережах, які варто знати та сповідувати навіть широким колам українських громадян.

Зокрема, у Telegram не варто підписуватися на анонімні канали, оскільки достеменно невідомо, хто їх автор, яка його позиція тощо. Часто у таких каналах поширюються чутки або неперевірена, емоційно заряджена інформація, мета якої змусити вас підписатися на цей канал. Іншими словами, клікбейт. Якщо ви читаєте новини в Телеграмі, можна орієнтуватися на канали медіа з білого списку Інституту масової інформації. Ці медіа є найякіснішими за результатами моніторингу, дотримуються стандартів журналістики та прозорості. Зокрема, це Суспільне, Громадське, Ліга, Українська правда, Укрінформ, ZN.ua, Бабель, НВ та Еспресо. Це саме стосується сторінок цих ЗМІ на інших платформах і в інших соціальних мережах, фейсбуці, ютюбі й твіттері.

Якщо ви все ж читаєте новини в Telegram, то варто обирати канали зі списку безпечних джерел інформації або ж “білого списку”, сформованого Центром протидії дезінформації.

Соціальні мережі є місцем поширення ботів та тролів. Особливо це актуально для фейсбуку та твіттера. Троль, скоріше за все, реальна людина і користувач, а бот – програма. Зазвичай сторінки ботів і тролів складаються з репостів інформації політичного або емоційного характеру, в них мало або й узагалі немає власних постів. Особиста інформація на їх сторінках зазвичай відсутня, а на аватарці акаунту поміщена картинка, взята з фотобанків або інших стокових джерел. Мета ботів і тролів – поширювати інформацію, аби надати їй ваги, важливості та публічного розголосу. Також вони активно пишуть коментарі, які часто є агресивними. Особисті повідомлення, які вони можуть надсилати користувачам, часто є написаними наперед, не особистими.

Компанія Meta має фактчекінгову програму, аби протидіяти дезінформації у фейсбуці, інстаграмі та ватсапі. Meta співпрацює з більш ніж 90 незалежними факчекінговими організаціями у 60 країнах світу, котрі виявляють, перевіряють та оцінюють потенційно дезінформаційний контент. В Україні Meta співпрацює з Vox-Check та StopFake.

Фактчекери не видаляють вміст, облікові записи чи сторінки у соцмережах, а попереджають користувача про те, що перед ним – фейк чи маніпуляція. На допис, що містить дезінформацію, накладають попереджувальний ярлик із посиланням на звіт з перевіркою фактчекерів. Це стримує поширення дезінформаційного контенту та мінімізує кількість людей, які його побачать.

Також кожен користувач мережі може скаржитися на допис, що, на його думку, містить неправдиву чи маніпулятивну інформацію. В усіх соцмережах алгоритм подачі скарги схожий:

1. Натиснути на значок із трьома крапками (у фейсбуці, інстаграмі та твіттері він знаходиться у правому верхньому куті, на ютубі – у нижньому).
2. Обрати опцію «поскаржитися» та вказати причину.
3. Дотримуватись подальших вказівок для завершення процесу подачі скарги.

4.6 / ЯК АНАЛІЗУВАТИ МЕДІАРЕСУРСИ

Не всім медіаресурсам можна довіряти. Якщо новини з медіа одразу викликають у вас сильні емоції, наприклад, страх, то будьте обережні з таким ресурсом. Також одразу переконайтеся, що сайт є прозорим, тобто, надає всю інформацію про редакторів, власників, редакційну політику тощо.

Український Інститут масової інформації щороку готує список білих медіа, тобто, ЗМІ, які є найякіснішими за результатами їх моніторингу. Так, експерти аналізують, чи поширює ЗМІ маніпуляції, фейки, мову ворожнечі, матеріали з ознаками замовлення тощо. Також медіа перевіряють на дотримання стандартів журналістики та прозорості – наявності на сайті контактів, редакційної політики, даних про власника тощо.

Для перевірки нового та незнайомого для вас іноземного медіа варто використовувати ресурс Media Bias/Fact Check або Interactive Media Bias Chart. Ці ресурси показують рівень фактологічності та упередженості ЗМІ. Звісно, варто довіряти тим ЗМІ, які за результатами перевірки є найбільш неупередженими та об'єктивними.

5/
ЯК РЕАГУВАТИ НА ІНФОРМАЦІЙНУ ЗАГРОЗУ

5.1 / ОЦІНЮВАННЯ СИТУАЦІЇ

Аналіз інформаційної загрози. При потенційному зіткненні з інформаційною загрозою у будь-якому її вигляді: фейкові або маніпулятивні новини, активність ботів, сокпапетів чи фіктивних сайтів, потрапляння вашого прізвища на фейковий документ, або навіть зіткнення з фактом використання діпфейків – першим кроком завжди повинен бути аналіз ситуації. Це допоможе відреагувати на неї максимально ефективно.

Оцінка рівня інформаційної загрози. Найбільш ефективною є система оцінювання на основі балів.

Обсяг		***Джерело***		***Шкідливий вплив***	
Наскільки поширився наратив. Чи може він поширитися найближчим часом?		Наскільки великий вплив має джерело наративу на процес прийняття рішень щодо інтересів національної безпеки?		Якою мірою наратив? • Створює ризик для громадського порядку? • Створює ризик для здоров'я населення? • Створює ризик для вразливих груп, або меншин? • Чи впливає на здатність уряду функціонувати? • Чи вплине на міжнародну репутацію України?	
Дуже обмежене поширення/ залучення?	0 балів	Джерело не має впливу	0 балів	Ніякого шкідливого впливу	0 балів
Певна залученість серед нішевої аудиторії та бульбашка фільтрів/ автоматизоване поширення	1 бал	Джерело має вплив на ключові групи, чи регіони	1 бал	Дуже обмежений шкідливий вплив	1 бал
Популярне в Інтернеті, доповнене неросійськими активами, може включати вікриті дебати та спростування	2 бали	Джерело має вплив на всю країну	2 бали	Обмежений шкідливий вплив	2 бали
Деякі незначні репортажі в основних ЗМІ	3 бали	Джерело має вплив на сусідні країни	3 бали	Певний шкідливий вплив	3 бали
Головний інфопривід, що впливає на повсякденну роботу	4 бали	Джерело представляє офіційну позицію країни	4 бали	Високий шкідливий вплив	4 бали

Оцінка	***Рівень загрози***	***Приклад***
10-12 балів	Високий	Наприклад заява Міноборони Росії (24 червня 2021 року): «Попереджувальні постріли та скидання бомб на шляху HMS Defender в 12 милях від узбережжя Криму»
6-9 балів	Середній	Наприклад кілька кремлівських ЗМІ (травень 2021): «Роман Пратасевич воював разом з неонацистами у війні на Донбасі»
0-5 балів	Низький	Наприклад одиночний сюжет на Ukraina.ru (16 червня 2021): «Україна - маріонетка Заходу, яка створює проблеми Росії»

Фактчекінг. Він необхідний для того, щоб остаточно упевнитись, що ви маєте справу з дезінформацією. Детальний інструментарій для перевірки фактів наведено у розділі 4.

Знайдені у процесі фактчекінгу докази стануть вашими аргументами у комунікації з державними органами та аудиторією. Якщо інформаційна загроза стосується вас особисто або сфери вашої відповідальності – вам необхідно розробити тактику дії в цій ситуації, включно з комунікацією щодо такого факту. Якщо ви маєте справу з припиненням поширення фейків або дезінформації як особа, яка має контролювати певне інформаційне середовище – від будинкового чату або Твіттер-акаунту регіонального ЗМІ й до регіональної прес-служби найвищого рівня – ви маєте припиняти ворожу активність, блокуючи ворожі акаунти, видаляючи інформацію, фіксуючи кейс та повідомляючи компетентних представників центральної влади в Україні.

Журналісти можуть проводити перевірку самостійно або ж залучитись допомогою національних фактчекінгових організацій.
Місцева влада також може обрати співпрацю з медіа або фактчекерами.

5.2/ КОМУНІКАЦІЯ З НАСЕЛЕННЯМ ТА ДЕРЖАВОЮ

Після проведення оцінки загрози слід перейти до інформування. Це може бути як комунікація з населенням, так і послідовне та повне інформування зацікавлених органів влади для подальшої координації відповіді на загрозу, залежно від оцінки її міри впливу та можливих наслідків, а також пріоретизації їх впливовості.

«Просто про складне». Комунікація з населенням має бути максимально простою та доступною: читач відразу має побачити, що певна інформація – це фейк або маніпуляція. Наприклад, пост у соціальних мережах чи відеосюжет, який отримав велике розповсюдження в регіоні, має бути публічно прокоментований – чому це фейк, які ознаки фейку, якою є ситуація насправді в межах компетенції органу, який виголошує інформацію. Місцева влада може опублікувати відповідну заяву на своїх офіційних ресурсах: сайті, сторінках у соціальних мережах, сторінці відповідальної особи.

Спростіть доступ до інформації для вашої цільової аудиторії: організуйте заходи, зустрічі, пресконференції, щоб обговорити конкретну проблему.

Інформування зацікавлених сторін. Місцева влада також може підготувати офіційну заяву для колег, інших департаментів чи інших державних органів. Прокомунікуйте фактичні обставини справи у нейтральному вигляді, якщо йде мова про низький рівень загрози, який потребує реагування на рівні організації. Або ж підготуйте заяву, що ви досліджуєте ситуацію. Це дасть вам час на підготовку ретельнішої відповіді.

5.3/ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ У ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

Робота з наративами.
Російська пропагандистська машина невпинно штампує фейки, часто – на одну й ту саму тему. Тому коли ви зустрічаєтесь з фейком чи маніпуляцією від пропагандистів, вірогідно вони є частиною певного російського наративу на певну тему.

Наприклад, ЗМІ пишуть про «заборону опозиційних медіа», «заборону партії як переслідування опозиції», – ці маніпулятивні тези можна об'єднати в один наратив: «Україна – не демократія». Разом з ними до наративу про недемократичність України також належатимуть тези: «Україна порушує права національних меншин» або «В Україні придушується російська мова».

Наративи постійно видозмінюються, реактуалізуються, тобто в інформаційній повістці, нав'язуваній ворогом, різко "спалахують", мить, і "зникають" одні тези щодо одного певного наративу, і вже за кілька днів, залежно від обставин, може актуалізуватися інший. Утім, фахівці постійно ведуть спостереження за цими наративами, наративними моделями, методами їх поширення та конкретними прикладами. Саме тому ви можете спостерігати активну публічну діяльність фактчерерів, саме тому в щоденному і щогодинному режимів Центр Протидії Дезінформації РНБО та громадські організації відповідного профілю інформують українців про нові й нові фейки та маніпуляції росії. І кожен такий фейк або маніпуляцію можна класифікувати, тобто віднести до певного російського "наративу" щодо України.

Деякі наративи є фоновими, тобто вони постійно циркулюють в інформаційному просторі. Розуміння сенсів, закладених у наративи, а також зв'язок певних тез у маніпуляціях та наративу, який вони інформаційно "підсвічують" дозволить вам якісніше аналізувати ситуацію та поглиблювати комунікацію з населенням шляхом освітньої компоненти.

Окремі наративи російської пропаганди.
Оскільки повна сукупність є чутливою інформацією, а детальних аналіз навіть описаних нижче наративів зайняв би за обсягом ґрунтовну монографію, ми окреслюємо лише смислові поля основних наративів. За аналогією до такого аналізу, ви можете проаналізувати й інші сумнівні та фейкові твердження, що діють в українському інформаційному просторі в інтересах російської федерації як імперіалістичної держави. Ми наводимо приклади кокретних кейсів, описаних випадків, що ілюструють використання таких наративів. Для зручності роботи з інформацією – посилаємося на одну соціальну мережу, але ви могли переконатися з попередніх розділів, що аналогічним чином наративи функціонують і в інших соціальних мережах.

- **Україна торгує переданим їй озброєнням**

Вказаний наратив у медійному просторі зазвичай наповнюється наступними меседжами: «західні союзники України не здатні забезпечити належний контроль за озброєнням, переданим Україні», «передане Україні озброєння можна вільно купити у Darknet», «переданим Україні озброєнням воюють у багатьох сучасних «гарячих точках»», «іноземне озброєння, передане Україні почало з'являтися в міжнародних терористичних організаціях» тощо.

Приклади:
https://t.me/breakingmash/48416
https://t.me/MID_Russia/33720
https://t.me/aklintsevich/1653 (фейк)

- **Україна – центр чорної трансплантології**

Вказаний наратив у медійному просторі зазвичай наповнюється наступними меседжами: «тіла загиблих військових «розбирають» на органи у прифронтовій зоні», «чорні трасплантологи працюють під прикриттям міжнародних організацій», «Україна передає дітей чорним трансплантологам країн ЄС», «українська влада покриває діяльність чорних трансплантологів»

Приклади:
https://t.me/prigozhin_2023_tg/8144
https://t.me/sheyhtamir1974/66559
https://t.me/OstashkoNews/109025
https://t.me/AleksandrSemchenko/32772

- **Україна – штучно створене державне утворення**

Вказаний наратив у медійному просторі зазвичай наповнюється наступними меседжами: «Україна складається з окремих частин різних держав», «Україна створена Росією», «Україна є проєктом Леніна», «коли Україна розвалиться, інші держави повернуть собі власні історичні території» тощо.

Приклади:
https://t.me/bear007/44323
https://t.me/readovkaru/2437
https://t.me/AleksandrSemchenko/24936
https://t.me/dillfrash/30915

- **Україна – не демократія**

Вказаний наратив у медійному просторі зазвичай наповнюється наступними меседжами: «Українська влада проводить політичні чистки», «закони не для влади», «в Україні діє жорстка цензура», «свобода слова в Україні – ілюзія», «влада України знищує канонічне православ'я» тощо

Приклади:
https://t.me/skosoi/6315
https://t.me/ZeRada1/18398
https://t.me/absatzmedia/76106

- **Україна - центр проведення медичних та біологічних досліджень**

Вказаний наратив у медійному просторі зазвичай наповнюється наступними меседжами: «в українських лікарнях проводять експерименти над пацієнтами», «на українцях тестують експериментальні ліки західних фармакологічних компаній», «кров слов'ян, зібрану в Україні використовують для розробки нових видів біологічної зброї»,

«Україна є для США найбільшим полігоном для проведення дослідів над людьми» тощо

Приклади:
https://t.me/bio_genie/4566
https://t.me/voenkorKotenok/53926
https://t.me/bio_genie/4479

- **українці – нацисти**

Вказанийv наратив у медійному просторі зазвичай наповнюється наступними меседжами: «Україна проводить умисний геноцид власного народу», «військовослужбовці ЗСУ вчиняють військові злочини», «українська сторона використовує цивільне населення як живий щит», «українські військові застосовують хімічну зброю», «Україна обмежує права російськомовних громадян» тощо.

Приклади:
https://t.me/zovgrad/16567
https://t.me/sheyhtamir1974/74552
https://t.me/goryachiye_novosti/6102

- **українці прагнуть приєднатися до росії**

Вказаний наратив у медійному просторі зазвичай наповнюється наступними меседжами: «українці – «русские» люди», «українці – «совєцкіє» люди», «населення підконтрольних Києву територій, прагне возз'єднатися з РФ», «прихід росіян уже не здається простим людям чимось жахливим», «підтримка дій РФ серед українців зростає», «вибори на окупованих територіях – справжні, їхні результати – відповідають дійсності» тощо.

Приклади:
https://t.me/skosoi/6199
https://t.me/readovkanews/75286
https://t.me/smotri_media/73092

Залучення експертів.

При роботі з дезінформацією може знадобитись експертна думка, оскільки фейкороби обирають зокрема й досить вузькоспеціалізовані теми. Збір різних оцінок зробить вашу перевірку повнішою, що сприятиме формуванню довіри читача. Крім того, залучення фахівців різних галузей дозволить поширити ваше повідомлення на ширшу аудиторію.

5.4/ ЗАХОДИ ПРЯМОГО ВПЛИВУ НА ЗАГРОЗУ

Якщо ви переконалися у реальності загрози, зрозуміли, що вона належить до одного з ворожих наративів, а отже її потрібно усунути, ви можете обрати для цього один із запропонованих нижче методів прямого впливу на загрозу.

Скарги. Якщо шкідливий інформаційний вплив є результатом порушення законів держави або кодексу поведінки соціальної мережі, слід звертатися до правоохоронних органів або адміністрацій платформ з метою видалення публікацій. Таким інструментом не слід зловживати для уникнення негативних публічних дискусій.

Блокування. Шкідливий інформаційний вплив певного суб'єкта можете стати причиною його блокування на платформах. Проте таке блокування має бути чітко вмотивоване порушеннями правил платформ. Даний інструмент також несе ряд потенційних ризиків, головним з яких є популярність суб'єкта блокування та його репутація. Якщо він має бездоганну репутацію та є популярним, нічого не заважає йому або створити нову сторінку і швидко відновити аудиторію, або оскаржити рішення, що може стати причиною небажаних публічних обговорень.

Викриття. Викриття справжніх мотивів та цілей суб'єкта шкідливого інформаційного впливу. Розкриття деталей інформаційних кампаній, які він проводить, та їх скоординованості з ворожим актором. Є одним із найдієвіших інструментів реагування на великі кампанії з високим рівнем загрози. Однак є певні ризики, для уникнення яких викриття має бути підкріплене всебічним аналізом, який не залишає місця для спекуляцій.

6/ ВИСНОВКИ

Користуючись цим посібником, регіональні лідери думок та члени їхньої команди, відповідальні за комунікації, можуть значно підвищити свою спроможність виявляти, розпізнавати, аналізувати та реагувати адекватним чином на вороже втручання в український інформаційний простір.

Ви переконалися, що мільярди доларів, витрачені росією на пропаганду, спрямовуються зокрема й на роботу ботоферм, що просувають російські наративи в українському інформаційному просторі, тобто в тих ділянках соціальних мереж, які користуються популярність в українських користувачів, однак не модеруються достатньо строго.

Зокрема мова тут може йти й про регіональні групи та сторінки в соціальних мережах, регіональні форуми та чати, зокрема районні та будинкові. Інформаційна безпека в таких ділянках інфопростору, які також атакує російська пропаганда та дезінформація, є важливою складовою не лише регіональної, але й всеукраїнської безпеки та сталого розвитку.

Радимо ознайомити з цим посібником усіх причетних до інформаційної роботи з чутливими джерелами, зокрема з міжнародною інформацією у ваших організаціях. Також посібник буде важливим джерелом знань та навичок для журналістів, що ведуть дослідницьку роботу, для працівників прес-служб, модераторів веб-сайтів, сторінок у соціальних мережах, контент-менеджерів та SMM-менеджерів, працівників громадських організацій у сферах, пов'язаних з міжнародною інформацією, модераторів міських та регіональних, сільських форумів, чатів у месенджерах та груп у соціальних мережах.