

Іжутова І. В., кандидат наук з державного управління (0000-0002-2614-7014)

Інститут професійної військової освіти “Вишкіл Лідерів” Національного університету оборони України, Київ

Фейкові новини в малих групах соціальних мереж

Резюме. Інформаційна війна завжди починається до проведення військової операції, триває паралельно з нею та після її завершення. З 2014 року інформаційне середовище активно використовується Російською Федерацією для поширення пропаганди та дезінформації, а у 2022 році цей процес масштабувався та постійно зазнає змін та перетворень. На сьогодні агресор активно використовує малі групи в соціальних мережах для укорінення своїх нарративів, які він реалізовує через поширення фейків, дезінформації, негативної пропаганди, маніпуляцій тощо. У статті надані рекомендації щодо нівелювання негативного впливу.

Ключові слова: фейкові новини; стратегічні комунікації; інформаційні війна; нарратив; соціальні мережі.

Постановка проблеми. Численні дослідницькі проекти стосуються огляду теми поширення фейків, пропаганди, нарративів противника в інформаційному середовищі. Висувалися пропозиції щодо боротьби з неправдивою та фейковою інформацією, але немає досліджень саме використання малих груп в соціальних мережах для цього процесу. Інформаційне середовище в них перетворилося на справжнє поле бою за розум та серця аудиторій. Важливо точно розуміти підходи до його формування з метою побудови своєї проактивної на відміну від реактивної комунікації.

Аналіз останніх досліджень і публікацій. За минулі роки багато дослідників намагалися зробити свій внесок щодо питань, пов'язаних з розбудовою та становленням системи стратегічних комунікацій та соціальних мереж, загалом як частини всієї системи та елементу формування глобального інформаційного простору [1, 2], спроможностей стратегічних комунікацій, майже всі нормативні документи присвячені врегулюванню роботи традиційних медіа. На жаль, не досліджений механізм та підходи використання нових медіа в поширенні пропаганди. Саме період використання соціальних медіа на прикладі малих груп у соціальних мережах з 24 лютого 2022 року не розкритий та глибоко не проаналізований в останніх дослідженнях.

Мета статті – аналіз ведення інформаційної операції з боку Російської Федерації (далі – РФ) із використанням малих груп в соціальних мережах для обґрунтування рекомендацій щодо захисту інтересів національної безпеки та оборони шляхом побудови реактивної комунікації на локальному рівні.

Виклад основного матеріалу.

Пропозиція використання в інформаційному середовищі соціальних мереж постійно розширюється, збільшується як кількість самих платформ та месенджерів, так і розширюється палітра їх функцій. А це лише свідчить про тенденції формування та розвитку інформаційного середовища у відповідь на запити цільових аудиторій, які ретельно досліджуються та аналізуються.

Ті хто хочуть мати інформаційну перевагу, безумовно, враховують та відслідковують такі тенденції розвитку сучасного інформаційного середовища, появу нових каналів взаємодії з цільовими аудиторіями або просто аудиторіями, відчують їх потребу та інтереси. В підкріплення своїх давно сформованих нарративів РФ продукує величезну кількість різнопланової спотвореної інформації, якість якої буває різною: від низькопробної до ретельно продуманої брехні. Останнім часом активізована робота із наповненням інформаційного середовища України дідфейками, які продукує штучний інтелект. Створюються фейкові акаунти, неіснуючі сторінки у соціальних мережах бойових бригад або відомих людей тощо, які є “дієвим інструментом, бо вони проникають всередину українського суспільства”, стають вірусними [3]. Для їх поширення також активно використовуються малі групи (мікрогрупи) в соціальних мережах, які виступають в ролі “полігону” для таких повідомлень.

До таких малих груп відносяться прибудинкові чати, шкільні групи, робочі групи, групи батьківських колективів, групи мешканців району, мікрорайону, об'єднаної територіальної громади і так далі, які створюються на базі популярних в Україні

месенджерів, як-то “Viber” та “Telegram”, незважаючи на російське походження цих платформ (до 24 лютого 2022 року були рекомендації не використовувати ці платформи державним установам, але основне правило комунікацій – “працювати зі своїми аудиторіями і йти туди, де ці аудиторії присутні” – виконується, тому сьогодні в цих месенджерах з’явилися відомчі офіційні сторінки). Як правило, кількість учасників таких груп не є великою: від кількох десятків (сотень) до кількох тисяч. Вони призначені для полегшення комунікації з сусідами та батьками, всередині громад, мікрорайонів, житлових кварталів тощо. Зазвичай адміністраторами виступають ініціативні громадяни або уповноважені представники місцевої влади, якщо це є сторінки, задачею яких є інформування від імені керівництва громад. Усі їх учасники впевнені, що серед спільноти немає “чужих”, тобто в них зібрані або мешканці, або батьки, або колеги, або сусіди. Отже, в цих групах повинна панувати атмосфера взаємодовіри та розуміння. Уся інформація, яка там розміщується, контролюється та модерується адміністратором або адміністраторами і стосується виключно мети створення цієї групи. Але в такій групі раптом може з’явитися повідомлення на кшталт “Увага! Скоро буде обстріл” (а насправді немає навіть повітряної тривоги, немає небезпеки, але максимальне поширення по всіх групах створює паніку, а панічні настрої підсилюються, якщо таке повідомлення розміщується на сторінці певної посадової особи. Так в липні 2022 року активно через малі групи було розповсюджено повідомлення про масований ракетний обстріл, яке розмістив на своїй сторінці в Telegram-каналі голова Івано-Франківської міської ради, після чого поширилася паніка серед населення країни з посиланням на його канал і зазначенням, що навіть міський голова це підтверджує. Отже, мета повідомлення була досягнута і пропаганда спрацювала і простежила поширення свого повідомлення) або “Вторгнення зі сторони Білорусі вже готують” (активно цей меседж масштабувався в січні 2023 року шляхом передачі інсайдерської інформації від начебто військових, людей, які дотичні до розвідувальних органів, чим нагніталися панічні настрої та підвищувався рівень напруженості серед населення. Справді, серед населення було багато обговорень, що ось-ось буде напад, що робити, як захищатися, куди

бігти, а чи буде достатньо пального, щоб виїхати, а куди виїхати і т. ін.) тощо. Ці повідомлення поширюють для того, щоб створити паніку, для розділення та розшарування людей, для створення хаосу” [4]. Популярними є повідомлення, де викладена інформація з огляду на тиск на емоції читачів (це може бути заклик до допомоги пораненому бійцю в неіснуючому госпиталі, терміновий збір коштів, поширення певних провокативних повідомлень щодо справедливості подачі електроенергії до споживачів в умовах тощо), обов’язково є фраза на кшталт “обов’язково поширюйте, обов’язково перепост” – потім алгоритм соціальних мереж визначає коло вразливих абонентів, з якими можна “працювати” далі.

Спочатку подібні повідомлення можуть бути розміщені на фейкових акаунтах в інших соціальних мережах, потім шляхом перепосту вони з’являються в малих групах, де поки адміністратор зрозуміє, що відбувається, певна частина учасників вже побачить це повідомлення і поширить його далі, відправивши своїм рідним, друзям, колегам, знайомим, сусідам. Що відбувається далі?... Через постійний брак часу, перенасиченість інформацією, актуальність та доречність вибраної теми, читач швидко продиляється повідомлення, іноді навіть не задумуючись та не повністю розуміючи сенс повідомлення, пересилає повідомлення далі своїм рідним, друзям та знайомим, в інші групи (тому що кожен / кожна є учасником / учасницею не лише однієї групи), щоб поділитися новиною. І так ланцюгова реакція – інформація масштабується із невеликої групи до цілого регіону або країни. У цьому і полягає небезпека – повідомлення стає вірусним і ще довго переходить з однієї інформаційної платформи на іншу.

Так, у 2022 році після масштабних обстрілів об’єктів критичної інфраструктури, наслідком яких стали перебої з подачею електроенергії по всій країні із запровадженням графіків та віялового відключення електроенергії, через малі групи була запущена тема, що “поки країна без електроенергії, влада продає її в Європу” [5]. Час запуску повідомлення був обраний дуже вдало, коли населення країни було в суцільному стресі, занурившись в темряву, маючи перебої із доступом до мережі Інтернет, перебої з мобільним зв’язком і так далі, не маючи достатньо часу для перевірки інформації і коли в сусідньому будинку світло виключалося на пару годин, а в своєму немає

вже майже добу. Саме в цей час “спостерігаються динамічні феномени в інформаційному просторі, схожі на циклічні емоційні реакції в натовпі, що посилюють тривогу (тривожні вири та ін.)” [6]. В умовах погано Інтернет-з’єднання повідомлення в Telegram-каналах завантажуються швидше, ніж в інших соціальних мережах або месенджерах, тому саме в них спочатку на пропагандистських каналах розміщувалася “зрадницька” інформація, яка через агентів впливу в малих групах поширювалася на більші аудиторії, а потім вже ці повідомлення з’являлися на популярних українських Telegram-каналах з посиланням на обговорення в соціальних мережах.

Автор інформації знайшов слабе місце аудиторій і вплинув на їх емоції, спрямувавши реакцію в потрібний напрям, вигадуючи все нові і нові нісенітниці: “приправити” всю цю “кремлівську кашу” вирішили черговою “зрадою” – мовляв, у той час як українці страждають без “світла, води й тепла”, українська влада продовжує експортувати електроенергію за кордон і заробляти “у свою кишеню” [7].

Інформація настільки швидко та обширно ширилася, що виросла з малих груп до національних масштабів, що потребувало реагування на найвищому рівні. Тут спрацював підхід стратегічних комунікацій і максимально на вищих рівнях було надано коментарі та пояснення того, що насправді відбувається, але коли інформація так глибоко поширилася, вже важче зменшити градус напруги, краще попередити її поширення – застосовувати проактивний підхід в комунікаціях.

Таких прикладів викидів через малі групи є дуже багато, всі ці повідомлення стають вірусними і активно поширюються. Як правило, розміщують їх особи без фото або з дивними картинками (аватарками) замість них, з вигаданими іменами, часто є непримітними, поки в групі не знайдеться свідомий громадянин /громадянка, який / яка поставить під сумнів розміщене повідомлення. І справді, це спрацює: як тільки хтось надає грамотне пояснення такому повідомленню, але не вступає в сварку або суперечності з аудиторією, не ображає аудиторію, сенс роботи пропагандиста втрачається, і він зникає з групи зовсім або завмирає на якийсь час. У зовсім малих групах такого учасника легко вирахувати та видалити з групи, в більших групах це є проблемою.

Такі пропагандисти долучилися до груп за декілька місяців до початку широкомасштабної збройної агресії РФ проти України. Цього часу їм вистачило для ретельного вивчення аудиторій для винайдення тріщин у комунікаціях, невирішених проблем, на яких можна “грати”, уразливості цих аудиторій. За цей час вони протестували теми, визначили тих учасників, з якими можна працювати, які не є стійкими і через вплив на їхні емоції, болючі теми можна просувати потрібний контент. Навіть активно створювалися групи-клони [8]. Результатом їх роботи стало формування так званого “ударного” контенту. Під час виникнення кризових ситуацій людина діє за емоціями, а іноді з поля зору уходять деталі, увага не приділяється важливим елементам. Тому противник активно використовує такий момент для поширення своїх меседжів та пропаганди. В умовах паніки здатність об’єктивно сприймати інформацію притуплюється, бажання просто отримати інформацію привалює над її аналізом, а брак часу іноді не дозволяє роздивитися логотип групи, продивитися контент, який там поширюється. У найкритичніші періоди з початку широкомасштабної збройної агресії Росія через свої інформаційно-психологічні групи створили групи-клони в соціальних мережах, зокрема клонувалися групи невеликих населених пунктів, громад, які знаходилися в безпосередній близькості до бойових дій або російських військ, які стрімко просувалися територією Україною у лютому-березні 2022 року. Такі групи позначалися або невеликим прапором Росії, або мали інші майже непомітні позначки, які вказували на приналежність таких груп російській пропагандистській машині. Завдяки свідомим громадянам, які були присутні в таких групах, завдяки рівню їх критичного мислення, ці групи були швидко ідентифіковані, подані скарги у відповідні служби з метою їх блокування або видалення.

Задачею цих груп було формування інформаційного середовища, сприятливого для ведення безпосередньо бойових дій та початку операцій противником, а також зменшення довіри владі, порушення існуючого порядку в громадах. Так, дуже багато неправдивих повідомлень, які поширювалися в таких групах, стосувалися евакуаційних автобусів, які насправді не існували, або пересування неіснуючих колон техніки противника, після ракетних обстрілів піднімалося питання про наслідки влучення

ракет або бомб, щоб коригувати свої дії. Задача цієї інформації – паніка, відстеження розповсюдження інформації, фактичне введення в оману, збір даних (зокрема, коли групи створювалися в місцевості, де розташовані військові підрозділи). Головне, звісно, паніка – коли критичне мислення нівелюється, і людина починає діяти хаотично, а потім, заспокоївшись, намагається знайти винних. Як правило, на її думку, винна місцева влада, яка неправильно поінформувала, неправильно організувала евакуацію і так далі – у такій ситуації ніхто не думає, хто став джерелом поширення такої інформації і хто насправді винний. Або агенти противника роблять повідомлення про необхідність збору даних про місця влучання та ступень руйнування внаслідок ракетних атак або артилерійських обстрілів противником. Протягом кількох тижнів з початку широкомасштабної збройної агресії активність створення груп-клонів, активність агентів противника в місцевих групах була максимальною, потім вона пересунулася до регіонів, близьких до лінії фронту.

Як виглядають такі агенти в групі: це класичні тролі із зазначенням лише одного імені або вони зареєстровані під неіснуючим іменем, їх профіль не має фото. У принципі, вони не є помітними, тим більше в групах в месенджерах. Спочатку вони просто додаються в групу і спостерігають, визначають слабкі місця груп, не проявляють жодної активності. А в цих групах час від часу може бути присутня повністю різна інформація, яку такий агент збирає, узагальнює, формує певний профіль групи, визначає сильні та слабкі риси групи, які можуть бути використані для поширення певної інформації. За наявності, принаймні, одного-двох громадян, які звертають уваги на деталі, звикли перевіряти інформацію, робота таких агентів зводиться нанівець, оскільки їх повідомлення дуже швидко ідентифікуються і надається правдива інформація з посиланнями на реальні факти та події. Якщо ж група дуже легко керується маніпулятивними повідомленнями, то можна і створити повністю клоновану групу, для насичення інформацією в інтересах противника.

Набутий досвід активного використання малих груп соціальних мереж, зокрема протягом останніх двох років, є цікавим, унікальним і не є вичерпним.

На жаль, ця тематика не береться до уваги, зокрема на локальному рівні. Якщо ретельно моніторити такі групи на

локальному рівні, можна ідентифікувати “зародження”, або початкові етапи інформаційної операції противника, щоб попередити перехід до наступних етапів інформаційної операції, придушивши “зародки” дезінформації на цьому рівні. Такий підхід зменшить обсяги зусиль, необхідних для боротьби з дезінформацією. Загалом, основа має бути в проактивності та стійкості суспільства до такої інформації.

Рекомендації стосовно нівелювання негативного впливу:

по-перше, медіа освіта та просвіта громадян, максимальна робота з ними для пояснення технологій поширення інформації, громадянська свідомість – якщо учасники груп бачать явні ознаки пропаганди або дезінформації, не діяти на емоціях, спокійно і аргументовано пояснити, чому це неправдива інформація. Якщо в групі є хоча б одна людина, яка буде робити такі пояснення, до неї згодом долучатимуться інші учасники, а тоді робота провокатора буде марною і втратить сенс (фейкове повідомлення не масштабується);

по-друге, моніторинг таких малих груп – необхідні програмні засоби, які дудуть змогу вирішити цю проблему;

по-третє, робота з органами місцевого самоврядування. Найчастіше пропаганда вкорінюється в тих регіонах і місцевостях, де багато літніх людей, людей, які не працюють, або працюють в своїх громадах, тому більше часу виділяють спілкуванню в таких малих групах. На своєму локальному рівні вони повинні знати болючі теми громад, де є певні тріщини в контенті і закривати ці тріщини, інакше їх заповнить хтось інший.

Висновки. Отже, питання роботи з цільовими аудиторіями в соціальних мережах є актуальним та важливим, раннє виявлення та локалізація інформаційних вкидів дасть змогу уникнути масштабування повідомлень по всій території держави. На сьогодні значення роботи в них з метою припинення поширення неправдивої маніпулятивної інформації на рівні малих груп не ведеться і це є проблемою.

Напрями подальших досліджень. Це дослідження, яке стосується використання соціальних мереж для укорінення нарративів та меседжів противника, є другим. Перше стосувалося використання пропагандистських Telegram-каналів для сіяння паніки та формування настроїв серед населення України. Надалі дослідження буде продовжено у напрямку виявлення та уточнення підходів, які використовуються для

формування інформаційного простору та розвитку необхідного інструментарію для формування проактивної комунікації. Це дослідження не є вичерпним і буде розвинуте в майбутньому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації / Д. Дубов. URL: https://shron1.chtyvo.org.ua/Dubov_Dmytro/Stratehichni_komunikatsii_problem_y_kontseptualizatsii_ta_praktychnoi_realizatsii.pdf? (дата звернення: 08.10.2023).
2. Стратегічні комунікації для безпекових і державних інституцій : практ. посіб. / Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин ; за заг. ред. О. Давліканової, Л. Компанцевої. Київ : ТОВ "ВІСТКА", 2022. 217 с.
3. Кремлівська пастка: як пропаганда РФ імітує українських військових у соцмережах. 15 березня 2023 року. URL: <https://www.radiosvoboda.org/a/tiktok-viyskovi-propaganda-rosiyi/32319282.html> (дата звернення: 19.10.2023).
4. Як протидіяти російській пропаганді в соцмережах: інтерв'ю з комунікаційницею з Чернівців. 9 грудня 2022 року. URL: <https://suspilne.media/334406-ak-protidiati-rosijskij-propagandi-v-socmerezah-intervu-z-komunikacijniceu-z-cernivciv/> (дата звернення: 19.10.2023).
5. Перевірка фейків у рамках партнерства з Meta. 15 грудня 2022 року. URL: <https://voxukraine.org/nepravda-ukrayina-prodaye-elektroenergiyu-inshym-krayinam> (дата звернення: 19.10.2023).
6. Найдьонова Л. Медіапсихологія війни як основа концептуальних трансформацій медіаосвіти: від медіатравми до травмаінформованих практик // Проблеми політичної психології : зб. наук. праць. 2022. Вип. 12 (26). С. 173–197.
7. "Без світла і без вас". Як російська армія і пропаганда намагаються знищити енергетичну систему України. 12 грудня 2022 року. URL: <https://ms.detector.media/trendi/post/30826/2022-12-12-bez-svitla-i-bez-vas-yak-rosiyska-armiya-i-propaganda-namagayutsya-znyshchyty-energetychnu-systemu-ukrainy/> (дата звернення: 19.10.2023).
8. Телеграм-окупація. Як Росія вибудувала медіамережу, а вийшло потьомкінське село. 29 жовтня 2022 року. URL: https://texty.org.ua/projects/108016/telehram-okupaciya-yak-rosiya-vybudovuvala-mediamera-zhuvyishlo-potomkinske-selo/?src=read_next_banner&from=109498 (дата звернення: 19.10.2023).

Стаття надійшла до редакційної колегії 20.11.2023

Fake news in small groups of social networks

Annotation

Information warfare always begins before a military operation, continues in parallel with it and after it is over. Since 2014, the information environment has been actively used by the Russian Federation to spread propaganda and disinformation, and in 2022 this process has scaled up and is constantly changing and transforming. Today, the aggressor is actively using small groups on social media to perpetuate its narratives, which it implements through the spread of fakes, disinformation, negative propaganda, manipulation, etc.

The purpose of the article is to analyse the information operation conducted by the Russian Federation with the use of small groups in social media in order to substantiate recommendations for protecting the interests of national security and defence by building reactive communication at the local level.

Recommendations are made to mitigate the negative impact.

Firstly, media education and awareness of citizens, maximum work with them to explain information dissemination technologies, civic consciousness – if group members see clear signs of propaganda or disinformation, do not act on emotions, calmly and reasonably explain why this is false information. If there is at least one person in the group who makes such explanations, other participants will subsequently join in, and then the provocateur's work will be useless and lose its meaning.

Second, monitoring of such small groups - software tools are needed to solve this problem.

Third, work with local governments. Most often, advocacy takes root in those regions and localities where there are many older people who are not working or working in their communities, so they spend more time communicating in such small groups. At their local level, they need to know the painful topics of the communities where there are certain cracks in the content and close these cracks, otherwise someone else will fill them.

Keywords: fake news; strategic communications; information warfare; narrative; social media.