УДК 004.77, 355.1, 355.4 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/35-43

Прокопенко О. С., доктор філософії (0000-0002-5482-0317)
Федорієнко В. А., кандидат технічних наук (0000-0002-0921-3390)
Кульчицький О. С. (0000-0002-4901-0192)

Навчально-науковий центр стратегічних комунікацій у сфері забезпечення національної безпеки та оборони Національного університету оборони України, Київ

Підхід щодо виявлення і аналізу інформаційних загроз національній безпеці України у системі стратегічних комунікацій

Резюме. Розглянуті певні питання побудови системи управління стратегічними комунікаціями і запропоновано методичний підхід щодо своєчасного виявлення, аналізу та оцінювання інформаційних загроз національній безпеці України.

Ключові слова: стратегічні комунікації; інформаційний простір; наратив; інформаційна загроза; негативний інформаційний вплив; моніторинг інформаційного простору.

Постановка проблеми. Умови існуючого сьогодення характеризуються стадією становлення глобального інформаційного простору, революційною ознакою якого є використання інформації як засобу досягнення бажаної мети. Це досягається завдяки активізації процесів розвитку інформаційних технологій, для задоволення комунікаційних потреб у політичній, економічній, військовій, соціальній та інших сферах діяльності людства. Водночас, інформаційна відкритість світу об'єктивно сприяє проведенню інформаційних атак (операцій), що у даному контексті характеризує інформацію як зброю. Викладення інформації у необхідний на користь організатора інформаційної пропаганди спосіб, дозволяє формувати у суспільстві потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, тощо.

В умовах повномасштабної війни з Російською Федерацією (РФ) особливо актуальним постає питання інформаційної безпеки – одного з ключових чинників національної безпеки України. З 2014 року Україна стикається з безпрецедентним обсягом інформаційних атак, спрямованих на підрив державності, демократії, суверенітету та територіальної цілісності України. Найбільш значущими видами інформаційних загроз для України, яку поширюють Російські державні ЗМІ, проросійськи налаштовані агенти впливу через соціальні мережі і інші комунікативні канали, є спотворення інформації у вигляді відкритої пропаганди, інформаційного тероризму та дезінформації. При цьому, ціллю формування негативного образу, висвітлення у світовому сприйнятті України, як нестабільної, корумпованої та неспроможної до реформ держави. Негативний інформаційно-психологічний вплив спрямований на психологічну деморалізацію українського населення, посилення соціально-політичної поляризації, поглиблення розбрату між Україною та її західними партнерами.

Існуючі виклики і загрози національній безпеці України, обумовлюють необхідність проведення комплексу ефективних заходів для реалізації державних стратегічних наративів, а також своєчасної інформаційної протидії, нейтралізації деструктивного інформаційного впливу і підвищення інформаційної безпеки особистості, суспільства і держави.

Довідка. *Стратегічний наратив* – основоположна ідея, що відображає та визначає базові принципи існування та розвитку держави (її інституції), характер і спрямованість внутрішніх і зовнішніх взаємовідносин, на основі якої формуються напрямки реалізації державної (відомчої) політики [1].

З огляду на вищезазначене, значна роль в інформаційній протидії противнику належить оцінюванню інформаційного простору у системі стратегічних комунікацій, основу якого становить моніторинг. Застосування у моніторингу інформаційного простору сучасних теоретичних підходів та інформаційних технологій дозволить суттєво покращити виявлення та аналіз інформаційних загроз національній безпеці України.

Аналіз останніх досліджень і публікацій. Аналіз зарубіжних та вітчизняних джерел, відносно теорії і практики використання технологій моніторингу інформаційного простору, методів оцінювання інформаційного простору для виявлення

інформаційних загроз, а також проведення досліджень у окремих галузях моніторингу, як, наприклад, розвідка на основі відкритих джерел (Open Source Intelligence, OSINT), показує невпинність зростання інтересу до цієї галузі знань.

Проблематику інформаційних воєн, інформаційної безпеки у теорії комунікацій і моніторингу інформаційного простору досліджували вітчизняні вчені роботах [2-14].

Методологічні основи інформаційної безпеки, розгляд інформаційних воєн, як джерела загроз національній безпеці держави і воєнно-теоретичних аспектів інформаційної боротьбі висвітлено у роботах [2–6].

Класифікація і оцінка інформаційних загроз, негативного інформаційно-психологічного впливу, питань виявлення інформаційних операцій на основі аналізу інформаційного простору за результатами моніторингу, досліджено у роботах [7–11].

Питання, пов'язані з удосконаленням системи стратегічних комунікацій для забезпечення інформаційної безпеки України у воєнній сфері, обґрунтуванням умов функціонування системи стратегічних комунікацій, а також фактори, що створюють перешкоди на шляху створення нових комунікативних можливостей досліджено у роботах [12–14].

Аналіз наведених вище джерел надає змістовне уявлення загальнотеоретичних положень щодо підвищення ефективності і вирішення спектру завдань для забезпечення інформаційної безпеки держави у воєнній сфері, ефективного функціонування системи стратегічних комунікацій Міністерства оборони і Збройних Сил України. Проте, запропоновані теоретичні підходи щодо класифікації і оцінки інформаційних загроз за результатами моніторингу інформаційного простору не враховують специфіки їх використання у системі стратегічних комунікацій в умовах широкомасштабного вторгнення і розгорнутої інформаційної війни РФ проти України. Недостатньо уваги приділено класифікації інформаційних загроз національній безпеці України за у системі стратегічних комунікацій, зокрема, виявлення ворожих наративів РФ проти України. Водночас, потребує доопрацювання підходів до визначення успішності реалізації заходів протидії негативному інформаційно-психологічному впливу противника, а також до застосування сучасних інформаційних технологій і передових методів обробки текстового інформаційного контенту для підвищення обґрунтованості та оперативності прийняття рішень.

Мета статті – методичний підхід до моніторингу інформаційного простору для своєчасного виявлення і аналізу інформаційних загроз національній безпеці держави у системі стратегічних комунікацій на основі використання сучасних інформаційних технологій.

Виклад основного матеріалу. Головним завданням стратегічних комунікацій (СК) є скоординоване і належне використання комунікативних можливостей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави. [1]

Виходячи з вищевикладеного, складовими частинами (елементами) стратегічних комунікацій є: ініціатор комунікацій, адресат або цільова аудиторія, подання інформації та зворотний зв'язок із цільовою аудиторією. Розглядаючи управління стратегічними комунікаціями, як складну систему, можна виділити її наступні складові елементи наведені на схемі (рис. 1).

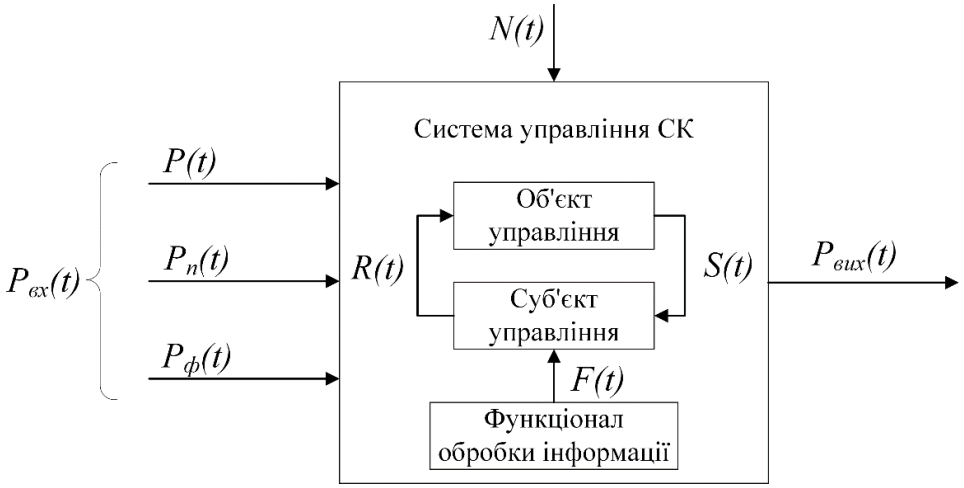

Рис. 1. Узагальнена схема управління стратегічними комунікаціями

Об'єктом управління (ОУ) або об'єктом інформаційного впливу може виступати особистість, певна цільова аудиторія, суспільство або держава.

Цільова аудиторія – це група людей, об'єднаних загальними ознаками. Це можуть бути представники однієї статі, віку, професії, соціального статусу, тощо.

Суб'єкт управління (СУ) – керівний склад Міністерства оборони і Генерального штабу Збройних Сил України, органи військового управління Міністерства оборони і Генерального штабу Збройних Сил України, а також організаційні структури, що здійснюють функції контролю реалізації заходів інформаційної політики.

Інформаційна політика (ІП) – це сукупність основних напрямів і способів діяльності по одержанню, використанню, поширенню та зберіганню інформації [15].

До вхідних інформаційних потоків системи управління СК, які здійснюють вплив на конкретний час – t, можна виокремити наступні:

$P(t)$ – інформаційні ресурси (текстовий, аудіо і відео інформаційний контент), що знаходиться у інформаційному просторі, джерелами якого можуть виступати веб сторінки глобальної мережі Інтернет, соціальні мережі, блогосфера, телебачення і радіо, тощо;

$P_n(t)$ – державна інформаційна політика, інформаційна політика Міністерства оборони України – сукупність інформації, яка визначає концептуальні засади, склад, структуру та стратегію розвитку СУ, у відповідності до імовірних сценаріїв застосування ОУ;

$P_ф(t)$ – фінансові потоки – інформація про рух грошових коштів, направлених на утримання і розвиток системи управління СК (програмно-технічне забезпечення).

Вхідний інформаційний потік на систему управління СК – $P_{вх}(t)$, можна відобразити у вигляді кортежу:

$$P_{вх}(t) = \langle P, P_n, P_ф, t \rangle. \quad (1)$$

Одночасно, на систему управління СК здійснюється негативний (деструктивний) інформаційно-психологічний вплив противника – $N(t)$, у вигляді проведення спеціальних інформаційно-психологічних заходів, акцій, операцій, кампаній, спрямованих на дестабілізацію реалізації заходів державної інформаційної політики.

Негативний інформаційно-психологічний вплив (ІПВ) – це, насамперед, маніпулятивні впливи на особистість, її емоційно-вольову сферу, на групову і масову свідомість, інструмент психологічного тиску з метою явного чи прихованого спонукання індивідуальних і соціальних суб'єктів до дій на шкоду власним інтересам на користь окремих осіб, груп чи організацій, що здійснюють ці впливи [3–6].

Контроль реалізації заходів ІП (ступінь реалізації комунікативних можливостей), а також наслідки негативного ІПВ $N(t)$, де суб'єктом управління аналізується стан ОУ – $S(t)$.

Вплив СУ на ОУ здійснюється шляхом реалізації (коригування) заходів ІП, а також заходів протидії негативному ІПВ – $R(t)$.

Вихідний потік системи управління СК – $P_{вих}(t)$, утворюється за рахунок обробки вхідних та внутрішніх інформаційних потоків функціоналом системи – F:

$$P_{вих}(t) = \langle P_{вх}, N, S, R, F, t \rangle. \quad (2)$$

Під функціоналом – F, системи управління СК, розуміють стійку впорядковану сукупність функцій (операцій) щодо вироблення і реалізації інформаційних, організаційних і розпорядчих заходів СУ, за результатами моніторингу інформаційного простору:

$$F = \{f_1, f_2, \dots, f_\mu\} \mid \mu \in \mathbb{N}, \quad (3)$$

де μ – індекс кількості виконуваних функцій;

$\mathbb{N}$ – натуральний ряд чисел.

Моніторинг інформаційного простору [16] – постійне спостереження за подіями та комунікаційними процесами в інформаційному просторі, збір та класифікація відповідної інформації для її подальшого аналізу, відслідковування основних тенденцій в інформаційному просторі, своєчасного виявлення інформаційних загроз та організації ефективної інформаційно-комунікаційної діяльності.

Функціонал системи управління СК включає:

- функції обліку і контролю поточного стану ОУ – добування, структурування, зберігання, пошук і тиражування даних;
- функції аналізу – аналіз стану реалізації заходів державної ІП, ІП Міністерства оборони України, виявлення в інформаційному просторі негативного ІПВ противника, ступінь його прояву, можливі наслідки, масштабність та джерела поширення;

- функції прогнозування – виявлення тенденцій розвитку державних та ворожих наративів, формування на основі статистичних даних прогнозних моделей щодо визначення значущості ворожої пропаганди за відповідними наративами: акція, спеціальна операція, кампанія;

- функції планування, організації і регулювання – вироблення інформаційних впливів по утриманню ОУ в існуючому стані або для його переведення в новий стан (вироблення управлінських рішень, заходи, та порядок їх реалізації у загальній системі управління).

Пріоритетними цілями та завданнями системи управління СК становить скоординоване і належне використання комунікативних можливостей, спрямованих на просування цілей держави. В свою чергу, спроможність у досягненні цілей управління на контрольну дату t визначаються показниками ефективності СК – $E(t)$, які входять до області значень відображення вихідного потоку параметрів у вигляді: $f_e: P_{\text{вих}} \to E$, отже:

$$E(t) = f_e(P_{\text{вих}}, t) = f_e(\langle P_{\text{вх}}, N, S, R, F\rangle, t). \quad (4)$$

Показники ефективності управління доцільно розглядати за складовими: організаційної, економічної та соціальної ефективності, які належать множині E, та представляють об'єднання попарно непересічних множин у вигляді:

$$E = \{E_o, E_e, E_s\}, \text{де: } E_o \cap E_e \cap E_s = \emptyset. \quad (5)$$

Організаційна ефективність E_o, включає показники, які визначають спроможність СУ:

- своєчасно реалізовувати комунікативні можливості до конкретної цільової аудиторії через конкретні канали комунікації;

- проводити якісний моніторинг інформаційного простору з метою встановлення стану реалізації заходів ІП, просування державних наративів, їх сприйняття суспільством;

- своєчасно виявляти, класифікувати і типізувати інформаційні загрози і ступінь їх прояву;

- реалізовувати заходи протидії і нейтралізації негативного інформаційного впливу.

Економічна ефективність E_e, включає показники, які визначають: поточні та прогнозні витрати на утримання СУ, а також забезпечення СУ всіма видами для гарантованого виконання функцій і завдань за призначенням.

Соціальна ефективність E_s, характеризується показниками, які відображають:

- посилення єдності, патріотизму, бойового духу, рівня мотивації, ступеню реалізації особистих потреб та вподобань ОУ;

- посилення віри у ОУ в обраному курсі держави, воєнно-політичного керівництва і складових сектору безпеки і оборони;

- формування у ОУ реального бачення перебігу подій зовнішньої і внутрішньої політики держави;

- формування у ОУ національної ідеї, культурних і духовних цінностей; зменшення рівня злочинності і корупційних проявів.

Складові ефективності системи управління СК мають притаманний кожній групі набір показників для їх розрахунку.

Наприклад, реалізація заходів протидії і нейтралізації негативного ІПВ противника за конкретною темою (наратив або складова частина наративу) (Табл. 1), що входить до групи показників організаційної ефективності приймає наступний вигляд:

$$E_{o_{ij}}(t) = N_{\text{н}_{ij}}(t) / N_{\text{в}_{ij}}(t), \quad (6)$$

де $N_{\text{н}_{ij}}$ – кількість нейтралізованих інформаційних загроз;

$N_{\text{в}_{ij}}$ – кількість виявлених інформаційних загроз;

i – індекс показника організаційної ефективності, де $i \in I$;

I – множина показників організаційної ефективності;

j – індекс теми, за яким класифіковано інформаційну загрозу, де $j \in J$;

J – множина тем;

t – контрольна дата.

Кожна тема, наведена у Табл. 1, на конкретний момент часу t може набирати свою гостроту, в залежності від цілей проведення інформаційної акції (операції) противника. Зазначене спостерігається за кількістю повідомлень по кожній темі, кількістю залучених до цього каналів розповсюдження інформації, тональності і інформаційного забарвлення повідомлень. Отже, окрема тема на момент часу t – матиме відповідний ваговий коефіцієнт, який визначається методом експертного оцінювання.

З цією метою, проводиться опитування групи з K експертів, де кожен залучений ε-*й* експерт, на основі особистої думки, виставляє чисельне значення рангу для кожної j-*ї* теми на момент часу t. Найбільш важливій темі

виставляється 1-*й* ранг, найменш важливій – значення рангу дорівнюватиме J. Таким чином, кожним ε-*м* експертом упорядковується важливість тем присвоєним значенням відповідного рангу.

Таблиця 1

Приклад класифікації текстового контенту з ознаками негативного ІПВ за темами

Назва кейса (процесу)	Назва теми
ДІЇ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ	Інформаційна політика Офісу Президента України
	Порушення свободи слова в Україні
	Залежність України від Західних країн
	Внутрішні протиріччя органів державної влади
	Корупція, махінації в органах державної влади
ІНФОРМАЦІЙНА ПОЛІТИКА ЗАХІДНИХ КРАЇН	Західні країни використовують Україну в своїх інтересах
	Західні країни "втомилися" від війни в Україні
	Західні режисери війни в Україні
	Скорочення військової, фінансової, гуманітарної допомоги Україні
КРИЗА В УКРАЇНІ	Енергетичний сектор
	Обстріли і руйнування цивільної і промислової інфраструктури
	Демографічна криза (внутрішньо-переміщені особи, виїзд з України)
	Екологічні проблеми
	Економічна криза
ПРОБЛЕМИ ЗБРОЙНИХ СИЛ УКРАЇНИ	Великі втрати особового складу в ЗС України
	Нехватка боєприпасів. Великі втрати озброєння і військової техніки
	Мобілізація через великі втрати особового складу
	Українська влада посилає бійців на смерть
	Невдалий контрнаступ ЗС України
	Некомпетентність, неправомірні дії (бездіяльність), тяжка хвороба (поранення) керівних посадових осіб Міністерства оборони і ЗС України
ПЕРЕГОВОРНИЙ ПРОЦЕС	Переговорний процес з Західними країнами і міжнародними організаціями
	Переговори з РФ не відбудуться. Небажання української влади вести переговори з РФ.
	Намагання РФ залучити Україну до переговорів для найшвидшого закінчення війни
ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА РОСІЙСЬКОЇ ФЕДЕРАЦІЇ	Успіхи збройних сил РФ у "СВО"
	Залякування населення України тактичною ядерною зброєю, ударами крилатих і балістичних ракет по енергетичній інфраструктурі, центрах прийняття рішень, тощо
	Плани збройних сил РФ по захопленню території України, країн Європи, застосування ядерної зброї по центрах прийняття рішень Великобританії і США
	Велич і бойовий потенціал збройних сил РФ ("другої армії Світу")

Враховуючи, що між присвоєним кожній темі рангом і важливістю теми існує лінійна залежність, для подальших розрахунків вагових коефіцієнтів, необхідно провести процедуру масштабування, із визначенням коефіцієнта важливості j-*ї* теми, наданої ε-*м* експертом [17, 18]:

$$V_{j\varepsilon}(t) = 1 - \frac{R_{j\varepsilon}(t)-1}{J}, \quad (7)$$

де ε – індекс експерта, де $\varepsilon \in K$;

$R_{j\varepsilon}(t)$ – ранг j-*ї* теми, виставлений ε-*м* експертом, на момент часу *t*, де $R_{j\varepsilon} \in \mathbb{N}$;

$V_{j\varepsilon}(t)$ – коефіцієнт важливості j-*ї* теми, на момент часу *t*, на основі експертної думки ε-*го* експерта, де $V_{j\varepsilon}(t) = \overrightarrow{0,1}$;

$\mathbb{N}$ – натуральний ряд чисел.

В результаті проведеної процедури масштабування, формується матриця коефіцієнтів важливості розмірністю $j \times \varepsilon$, отриманої на основі експертної думки ε-*го* експерта, для кожної j-*ї* теми, на момент часу *t*.

Для приведення отриманих абсолютних значень показників у безрозмірне значення без втрати їх вагомості, проводиться процедура нормування. Дана процедура необхідна для оцінки зваженості кожної j-*ї* теми серед множини тем J.

Нормування матриці коефіцієнтів важливості здійснюється наступним чином:

$$\varphi_{j\varepsilon}(t) = \frac{V_{j\varepsilon}(t)}{\sum_{j=1}^{J} V_{j\varepsilon}(t)}, \quad (8)$$

де $\varphi_{j\varepsilon}(t)$ – нормоване значення j-*ї* теми, на

момент часу t, на основі експертної думки ε-*го* експерта.

В результаті проведеної процедури, формується матриця нормованих значень показників розмірністю $j \times \varepsilon$, де $\sum_{j=1}^{J} \varphi_{j\varepsilon}(t) = 1$.

Вагові коефіцієнти кожної j-*ї* теми на момент часу (t) становитимуть:

$$\varphi_j(t) = \frac{1}{K}\sum_{\varepsilon=1}^{K} \varphi_{j\varepsilon}(t), \quad (9)$$

де $\varphi_j(t)$ – ваговий коефіцієнт j-*ї* теми.

Отже, загальне значення i-*го* показника організаційної ефективності для всієї множини тем J, на конкретний час t, прийматиме вигляд:

$$E_{o_i}(t) = \prod_{j=1}^{J} E_{o_{ij}}{}^{\varphi_j}(t). \quad (10)$$

Аналогічним шляхом розраховуються вагові коефіцієнти для кожного показника організаційної ефективності, де загальне значення показників організаційної ефективності $E_o(t)$ прийматиме вигляд:

$$E_o(t) = \prod_{i=1}^{I} E_{o_i}{}^{\eta_i}(t) \times 100\%, \quad (11)$$

де η_i – ваговий коефіцієнт i-*го* показника організаційної ефективності E_{o_i}.

Результати управління вважаються позитивними при підвищенні показника організаційної ефективності, де:

$$E_o^*(t_\delta) > E_o(t_{\delta-1}) \mid \delta \in \mathbb{N},$$

де δ - індекс кількості циклів управління;

$\mathbb{N}$ - натуральний ряд чисел.

Розрахунки ефективності реалізації заходів протидії і нейтралізації негативного ІПВ противника, за наведеним вище прикладом були апробовані у табличному процесорі MS Excel.

В якості вхідних даних, було використано значення присвоєних рангів десяти актуальним темам, оцінених шістьма експертами, а також кількість виявлених і нейтралізованих інформаційних загроз по кожній конкретній темі на момент часу t.

Ознаки негативного ІПВ виявляються на основі аналізу контенту інформації, отриманої шляхом моніторингу інформаційного простору, який здійснюється за певними етапами:

1) підготовчий;
2) добування даних;
3) класифікація і типізація даних;
4) аналіз даних;
5) прийняття рішень.

На Рис. 2 висвітлено структурно-логічну схему моніторингу інформаційного простору, з метою виявлення негативного ІПВ та адекватного реагування на загрози.

На *першому* етапі, визначається цілі і завдання, які повинен вирішити моніторинг. При цьому враховується охоплення (масштабність) виконання завдань: географічні, соціальні, політичні, на які цільові аудиторії слід зосереджувати увагу, тощо. Визначаються обмеження досліджень (тематика досліджень) і обираються перелік інформаційних ресурсів, які підлягатимуть моніторингу: веб-сторінки, Telegram, Facebook, Instagram, Twitter, тощо. Отже, всі ключові особливості і завдання, які виконувались за аналізом попереднього моніторингу, можуть уточнятись для проведення наступного. Підставою для цього можуть слугувати нові ключові події в Україні і світі, посилення негативного ІПВ противника по окремим темам, поява нових ворожих наративів, тощо.

На *другому* етапі, визначаються правила обробки даних. Визначаються шляхи отримання даних з інформаційних ресурсів, наприклад, яка саме технологія парсингу даних, наприклад, web scraping, web crawling, буде використовуватись і яким чином її налаштовувати під кожен окремий інформаційний ресурс. Також, визначаються способи структуризації даних: у текстових файлах, пласких таблицях, датафреймах, реляційних або нереляційних базах даних. Як правило, структурована інформація розміщується у реляційних базах даних, яка містить основні типові поля: дата і час повідомлення, заголовок, автор повідомлення, текст повідомлення, хештеги, посилання на джерело повідомлення, посилання (лінки) на інші джерела, які присутні в основному тексті повідомлення, тощо. Таким чином, структуризація даних надає первинні представлення (кількісні показники) для проведення подальшого аналізу.

Парсинг –це метод швидкої обробки інформації, точніше синтаксичний аналіз даних, розміщених на веб-сторінках. Він використовується для оперативного опрацювання великої кількості текстів, цифр, зображень [19].

Третій етап є найбільш відповідальним, в ході якого виконується класифікація (відповідність) повідомлень за певними темами (Табл. 1), а також встановлюється тональність і семантика текстів повідомлень (типізація даних).

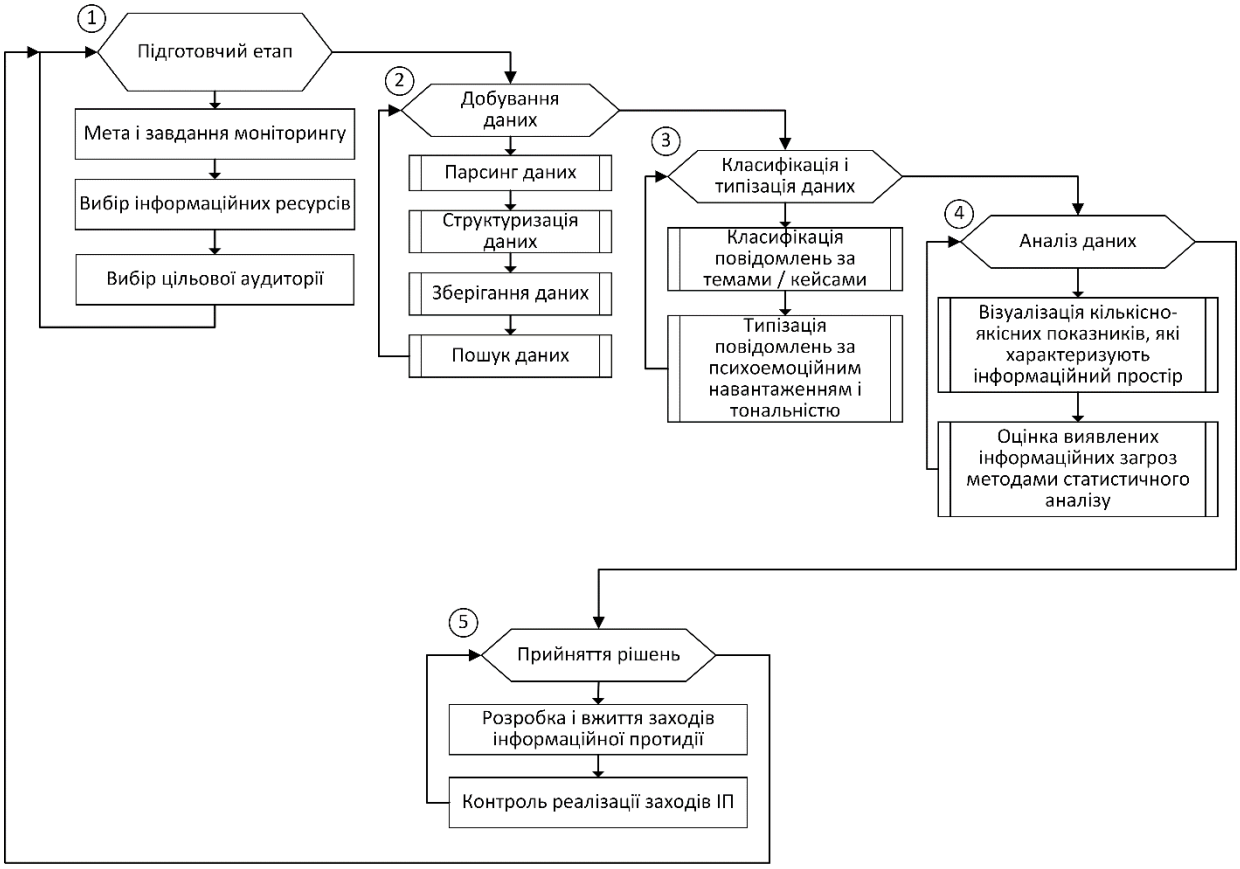

Рис. 2. Структурно-логічна схема моніторингу інформаційного простору

На сьогоднішній день, дана процедура виконується шляхом використання технологій машинного навчання (Machine Learning). Існує багато сервісів, призначених для аналізу семантики та структури текстового контенту, наприклад Gensim, FastText, SpaCy, TextRazor, Aylien та інші, які можуть бути використані для аналізу соціальних мереж, веб-сторінок та інших джерел інформації. Зазначене здійснюється на основі глибокого аналізу текстових даних для вилучення зв'язків, типізованих залежностей між словами та синонімами, створюючи своєрідні контекстно-семантичні конструкції. Наприклад, функції тематичного моделювання Gensim, на основі байєсівської моделі тематичного моделювання (Hierarchical Dirichlet Process), здійснює автоматизоване розпізнавання тематики текстового контенту. А на основі ймовірнісної моделі тематичного моделювання (Latent Dirichlet Allocation) – визначити кількість тематик та їх ключові слова. Інструментарій для збору та аналізу даних з соціальних мереж, які дозволяють відслідковувати обговорення певної теми в соціальних мережах. Такі інструменти, як: Social Mention, Netvibes та Hootsuite, можуть використовуватися для моніторингу репутації, виявлення інформаційних загроз та аналізу тенденцій у громадській думці. Наведені вище бібліотеки побудовані на базі платформи з відкритим кодом NLTK (Natural Language Toolkit) [20] для роботи з природними мовами. Вона надає доступ до корпусів текстів та лексичних ресурсів, а також має набір інструментів для обробки текстів, що допомагає вирішувати завдання, пов'язані з обробкою природних мов.

Якість отриманих показників значно підвищується, якщо для їх верифікації залучати широке кола експертів. Проте, зазначена процедура є найбільш трудомісткою і потребує витрати більшої кількості часу.

На *четвертому* етапі, проводиться аналіз кількісно-якісних показників, отриманих на попередніх двох етапах. З цією метою розробляються інтерактивні інформаційні панелі, на яких здійснюється їх візуалізація у вигляді графіків, діаграм, зведених таблиць, тощо. Зазначене, значно спрощує сприйняття інформації, дозволяє проводити аналіз тональності повідомлень і їх кількості за визначеними темами, проводити часові зрізи інформації.

Додатково досліджуються зміни інформаційного простору за визначений період на основі побудови статистичних моделей регресійного та кореляційного аналізу. Це дає змогу швидко оцінити критичні зони розвитку певної теми в

ретроспективі, ступінь активності певних джерел. Кореляція при цьому можлива між втратами противника, санкціями проти РФ, негативним інформаційним впливом противника тощо.

На основі отриманих статистичних моделей, формуються прогнозні аналітичні моделі можливого розвитку зміни інформаційного простору. Виявляються тренди розвитку певних тем та їх майбутня поведінка (за період до 30 діб). Використовуючи методи дослідження функції за ретроспективний період, існує можливість визначити початок інформаційних акцій (операцій) противника. Це сприяє підтримці прийняття обґрунтованих рішень і раціональному розподілу ресурсів залучених до протидії негативному ІПВ.

На *п'ятому* етапі, проводиться розробка і вжиття заходів щодо протидії негативному ІПВ, уточнення цілей і завдань моніторингу і контроль стану реалізації ІП.

Кожен описаний вище етап включає виконання ряду процедур, деталізувати які в рамках написання однієї статті неможливо. Водночас, систематизація знань про методи і способи, які використовують при моніторингу інформаційного простору, вказують на певну послідовність дій щодо комплексного уявлення цього процесу.

Висновок. Розглянуті у статті питання визначення показників ефективності системи управління стратегічними комунікаціями і запропонований методичний підхід щодо своєчасного виявлення, аналізу та оцінювання інформаційних загроз національній безпеці України, надає комплексне представлення щодо інформаційного супроводження діяльності уряду, державних інституцій і публічних осіб через комунікативні можливості держави. Інформаційна обізнаність цільової аудиторії про правильно обраний курс держави, державну інформаційну політику, інформаційну політику МО України забезпечує більш стійке просування стратегічних цілей держави. Ці функції набирають особливої актуальності під час розгорнутої проти України широкомасштабної збройної агресії, де крім проведення активних бойових дій, розгорнуто інформаційну війну. Зазначене вимагає застосування дієвих механізмів щодо виявлення, аналізу і прогнозування інформаційних загроз у інформаційному просторі.

Запропонований підхід щодо класифікації інформаційних загроз національній безпеці України у системи стратегічних комунікацій, визначення ефективності реалізації заходів інформаційної протидії і удосконалення процесу виявлення негативного ІПВ, може стати концептом для розроблення інформаційно-аналітичної системи моніторингу інформаційного простору, з подальшим її використанням в інформаційно-аналітичному забезпеченні органів військового управління, підрозділів Збройних Сил і Міністерства оборони України, на які покладаються зазначені функції. Це дозволить підвищити обґрунтованість рішень і ефективність вжиття заходів для протидії негативному інформаційно-психологічному впливу противника.

Подальші дослідження доцільно зосередити на деталізації етапів моніторингу інформаційного простору, методах на основі штучного інтелекту, які використовуються для класифікації і оцінювання інформаційних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України. Наказ Міністерства оборони України від 22.11.2017 № 612. – URL: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text (дата звернення: 21.08.2023).
2. Почепцов Г. Г. Информационные войны. Киев: Ваклер, 2000. – 576 с.
3. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): Монографія. Київ: НАОУ, 2003. – 320 с.
4. Жарков Я. М., Дзюба М. Т., Замаруєва І. В. Інформаційна безпека особистості, суспільства, держави: Підручник. Київ: Видавничо-поліграфічний центр "Київський університет", 2008. – 274 с.
5. Курбан О. В. Інформаційні війни у соціальних он-лайн-мережах : Монографія. Київ : ун-т ім. Б. Грінченка, 2017. – 392 с.
6. Інформаційна безпека держави у воєнній сфері: Навч. посібник / [.О. Кацалап, С.А. Микусь, О.В. Войтко та ін.]. Київ: НУОУ ім. І. Черняховського, 2020. − 304 с.
7. Додонов А.Г. Распознавание информационных операций/ А.Г. Додонов, Д.В. Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. Київ : ООО «Инжиниринг», 2017. – 282 с.
8. Сніцаренко П. М., Кацалап В. О. Методика оцінювання психологічного впливу. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ : НУОУ ім. І. Черняховського, 2018. № 3(33). – С. 113–118.
9. Сніцаренко П. М. Грицюк В. В. Аналіз стану виявлення та оцінювання негативного інформаційного впливу на особовий склад Збройних Сил України в системі протидії такому впливу. *Збірник наукових праць Центру воєнно-стратегічних досліджень.* Київ : НУОУ ім. І. Черняховського, 2019. № 2(66). – С. 52–61.

10. Кацалап В. О., Кирпічніков О. Д., Саунін Р. Д. Методичний підхід до оцінювання рівня інформаційно-психологічного впливу противника в інтересах інформаційної операції .Збройних Сил України. *Збірник наукових праць Центру воєнно-стратегічних досліджень.* Київ : НУОУ ім. І. Черняховського, 2022. № 3(76). – С. 24–31.
11. Федоренко Р. М. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері. *Сучасний захист інформації.* Київ, 2015. № 2. – С. 21–25.
12. Вербицька А. М., Савченко В. А., Дзюба Т. М., Кацалап В. О. Система стратегічних комунікацій Міністерства оборони України та Збройних Сил України. *Наука і оборона.* Київ, 2017. №1. – С. 9–12.
13. Войтко О., Кацалап В., Бабій Ю. Обґрунтування елементів комунікативної моделі системи стратегічних комунікацій Сил оборони. *Збірник наукових праць Національної академії Державної прикордонної служби України.* Хмельницький, 2019. № 2(80). – С. 61–72.
14. Войтко О. В. Оцінювання ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України. *Системи управління, навігації та зв'язку*. Київ, 2018. № 3(49). – С. 97–99.
15. Інформаційна політика. – URL: http://volynstandart.com.ua/information-policy/ (дата звернення: 21.08.2023).
16. Доктрина зі стратегічних комунікацій, затверджена Головнокомандувачем Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01. Київ, 2020. 32 с.
17. Загорка О. М., Мосов С. П., Сбітнєв А. І., Стужук П. І. Елементи дослідження складних систем військового призначення. Київ : НАОУ, 2005. – 100 с.
18. Денисов А. А., Колесников Д. Н. Теория больших систем управления: Учеб. пособие для вузов. Ленинград: Энергоиздат, 1982. – 288 с.
19. Що таке парсинг і для чого використовується? . – URL: https://dalistrategies.com/ua/shho-take-parsing-i-dlya-chogo-vikoristovuietsya/ (дата звернення: 21.08.2023).
20. Documentation. Natural Language Toolkit. – URL : https://www.nltk.org/ (дата звернення: 14.08.2023).

Стаття надійшла до редакційної колегії 25.08.2023

An approach to the identification and analysis of information threats to the national security of the state in strategic communications management systems

Annotation

The current conditions are characterized by the stage of formation of the global information space, the revolutionary feature of which is the use of information as a means of achieving the desired goal. This is achieved thanks to the activation of information technology development processes to meet communication needs in the political, economic, military, social and other spheres of human activity. At the same time, the information openness of the world objectively contributes to information attacks (operations), which in this context characterize information as a weapon. Presentation of information in a manner necessary for the benefit of the organizer of information propaganda allows forming the necessary point of view, public opinion, course of complementary logical thoughts, etc. in society.

In the conditions of a full-scale war with the Russian Federation, the issue of information security - one of the key factors of Ukraine's national security - becomes especially relevant. Since 2014, Ukraine has faced an unprecedented volume of information attacks aimed at undermining Ukraine's statehood, democracy, sovereignty, and territorial integrity. The most significant types of information threats to Ukraine, which are spread by Russian state media, pro-Russian agents of influence through social networks and other communication channels, are information distortion in the form of open propaganda, information terrorism and disinformation. The purpose of the mentioned is the formation of a negative image, highlighting in the world perception of Ukraine as an unstable, corrupt and incapable of reforms state. The negative informational and psychological influence is aimed at the psychological demoralization of the Ukrainian population, the strengthening of socio-political polarization, and the deepening of discord between Ukraine and its Western partners.

The existing challenges and threats to the national security of Ukraine necessitate the implementation of a complex of effective measures for the implementation of state strategic narratives, as well as timely informational countermeasures, neutralization of destructive informational influence, and increased informational security of the individual, society, and the state.

In view of the above, the resolution of this issue directly depends on the effectiveness of monitoring the information space and the application of modern approaches to the detection and analysis of information threats in the strategic communications system of the Ministry of Defense and the Armed Forces of Ukraine.

Keywords: strategic communications, information space, narrative, information threat, negative information impact, information impact analysis