безпекові вимоги реалізації блокчейн-технології. Зокрема, технології повинні мати якомога менше програмних вразливостей, що можуть бути використані зловмисником. Таким потенційно може бути будь-який новий член мережі. Проблема високих вимог до мережі частково вирішується формуванням довіреного кола вузлів, які будуть підтримувати блокчейн і не давати зловмисникам використовувати уразливості навіть за їх наявності.

Відкритість інформації в децентралізованих системах має позитивні наслідки для спільноти, проте є великі ризики розкриття адреси суб'єкта інформаційної діяльності. Аналіз наявних децентралізованих систем (наприклад, Bitcoin, Ethereum) засвідчує вразливість інформації на рівні ідентифікації приналежності окремих адрес конкретним суб'єктам інформаційного процесу. Тому для оптимальної безпекової інформаційної діяльності в системі оптимальним є використання мультипідпису або смартконтрактів.

Список використаних джерел

1. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin, 2016. 348 c.

2. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. 130 c.

3. Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley, 2016. 179 c.

4. Kulikovskyi A. Технологія blockchain як складова інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2019. Vol. 4(4). P. 85–89. https://doi.org/10.28925/2663-4023.2019.4.8589

Наместнік В. В., канд. наук з держ. упр.,
Національний університет оборони України імені Івана Черняховського,
м. Київ

СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В УМОВАХ ВОЄННОГО СТАНУ

Через з повномасштабну збройну агресію Росії проти України з 24 лютого 2022 року в Україні введено воєнний стан [3]. Це особливий правовий режим, в умовах якого на перше місце виходять питання національної безпеки держави, невід'ємним складником якої є інформаційна безпека. У Стратегії інформаційної безпеки [4] соціальні мережі згадуються в контексті глобальних загроз та викликів як суб'єкти впливу в інформаційному просторі. В умовах воєнного стану ця

загроза ще більше актуалізувалась, оскільки соціальні мережі стали одним із найпоширеніших джерел інформації в Україні. У глобальному вимірі лідером цього ринку є Facebook (Meta). Станом на січень 2022 року кількість користувачів цієї соцмережі перевищувала 2,91 мільярда [2]. Аналіз вітчизняного інформаційного простору вказує, що у 2022 році у відбулися суттєві зміни у структурі джерел інформації. За даними опитувань, 85 % українців щоденно використовують інтернет, 74 % опитаних вказали соціальні мережі як основне джерело отримання новин, а 60 % – довіряють новинам у соціальних мережах. За результатами цього ж опитування, у 2022 році значно зросла популярність використання Telegram. Він став основною соціальною мережею як для комунікації, так і для споживання новин [2].

Масове залучення авдиторії та висока швидкість поширення інформації сприяють тому, що соцмережі стали не лише зручним майданчиком комунікації, а й інструментом поширення маніпуляцій, дезінформації та пропаганди, зокрема російської. Слід зазначити, що російська пропаганда за допомогою соціальних мереж намагається конструювати не лише український, а й інформаційний простір інших держав. Найбільш агресивною є риторика щодо держав, які активно підтримують Україну та надають допомогу, – Східної Європи, Великої Британії, Німеччини та США.

Водночас ворог використовує соціальні мережі не лише для поширення пропаганди чи дезінформації, але й для психологічного тиску на українське суспільство: посилення паніки й страху, підриву довіри до дій влади та Сил оборони України, розділення українців на основі політичних чи релігійних уподобань, мовного питання тощо. У такий спосіб ворог намагається ще більше дестабілізувати ситуацію всередині нашої країни для досягнення власних інтересів.

Зараз на українську авдиторію орієнтуються тисячі телеграм-каналів із новинним, розважальним чи будь-яким іншим контентом. Станом на кінець 2022 року дослідники українського сегменту Telegram виокремили понад 300 каналів, що просували російські сповіщення в український інфопростір [1]. Здебільшого такі телеграм-канали є анонімними, проте частина з них чітко асоціюється з проросійськими особистостями (політиками, журналістами, блогерами, тощо). Особливістю Telegram є те, що постійно з’являються нові телеграм-канали, або ж наявні змінюють власника, й відповідно – риторику. Відслідкувати такі зміни можливо лише шляхом систематичного моніторингу великого масиву даних. Тож навести вичерпний список ворожих телеграм-каналів фактично неможливо. Часто телеграм-канали з проросійською риторикою мімікрують під українські телеграм-канали та приховано (маніпулятивно) просувають наративи російської пропаганди.

В умовах воєнного стану українці почали частіше звертатись до офіційних джерел інформації, зокрема до верифікованих сторінок представників влади чи

відомств у соціальних мережах. Тому російська пропаганда створює фейкові акаунти, що за стилем оформлення схожі на офіційні сторінки, для поширення неправдивої інформації. Протягом 2022–2023 років такі акаунти створювали від імені Валерія Залужного, народних депутатів України, компаній «Укренерго» та «ДТЕК», благодійного фонду «Повернись живим», підрозділів ЗСУ тощо. У такий спосіб ворог також намагається підірвати довіру до влади, лідерів думок та волонтерів.

Соціальні мережі під час повномасштабної війни слугують для ворога ще й джерелом розвідданих (OSINT-технології – Open Source Intelligence). Під впливом різних чинників (зокрема внаслідок вкрай збудженого емоційного стану) користувачі соцмереж публікують результати ворожих обстрілів або ж фото чи відео роботи української системи протиповітряної оборони. Такі дописи дають можливість ворогу дізнатись про результати їх роботи й коригувати подальші обстріли території України. Те саме стосується й поширення повідомлень, світлин та відеозаписів переміщення військової техніки ЗСУ. Слід також зазначити, що особисті сторінки військовослужбовців у соціальних мережах можуть слугувати джерелом для збору відомостей про особовий склад чи переміщення підрозділів української армії. Корисною для ворога може бути й інформація, яку поширюють родичі військовослужбовців у спільнотах чи на сторінках, присвячених пошуку безвісти зниклих військовослужбовців.

Після повномасштабного вторгнення Росії на територію України відбулася нова хвиля активізації українського волонтерського руху. Допомоги потребували як Сили оборони України, так і люди, що постраждали внаслідок повномасштабної збройної агресії. Велика кількість різноманітних волонтерських зборів стала прикриттям для шахраїв, котрі почали використовувати ситуацію для привласнення коштів чи викрадення персональних даних довірливих користувачів соціальних мереж.

Вирішенням проблеми деструктивного інформаційно-психологічного впливу соціальних мереж може слугувати підвищення рівня цифрової та медіаграмотності населення. Недостатній рівень медіаграмотності (медіакультури) українців визначений однією з глобальних загроз в інформаційному просторі [5].

Як свідчать дослідження [6], щороку зростає кількість людей, які користуються інтернетом, також зростає і загальнодоступність інтернету в Україні. Частково це сприяє зростанню рівня цифрової грамотності українців, проте проблема все ще зберігається. У Стратегії інформаційної безпеки [4] для вирішення цієї проблеми передбачено проведення просвітницьких кампаній з медіаграмотності, що сприятимуть розвитку критичного мислення, фактчекінгу (перевірки фактів) тощо.

Список використаних джерел

1. «Кремлівська гідра»: 300 телеграм-каналів, які отруюють український інфопростір. URL: https://detector.media/monitorynh-internetu/article/205954/2022-12-14-kremlivska-gidra-300-telegrm-kanaliv-yaki-otruyuyut-ukrainskyy-infoprostir/ (дата звернення: 26.05.2023).

2. Найпопулярніші соціальні мережі у світі станом на січень 2022. URL: http://google.com/amp/s/marketer.ua (дата звернення: 26.05.2023).

3. Про введення воєнного стану в Україні. Указ президента України № 64/2022 від 24 лютого 2022 року. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 26.05.2023).

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Указ президента України № 685/2021 від 28 грудня 2021 року. URL: https://www.president.gov.ua/documents/642022-413976852021-41069 (дата звернення: 26.05.2023).

5. Рівень цифрової грамотності українців: про що свідчить дослідження Мінцифри. URL: http://nrcu.gov.ua/news.html?newsID=97355 (дата звернення: 26.05.2023).

6.Українські медіа, ставлення та довіра у 2022 році. URL: https://internews.in.ua/wp-content/uploads/2022-11/Ukrainki-media-stavlennia-ta-dovira-2022.pdf (дата звернення: 26.05.2023).

Палій С. В., аспірант,
Київський національний університет культури і мистецтв, м. Київ

ПРОБЛЕМАТИКА ДІЯЛЬНОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ЦЕНТРІВ В УКРАЇНІ В УМОВАХ ВОЄННОЇ АГРЕСІЇ

Важливою умовою стабільної життєдіяльності суспільства за будь-яких обставин є усунення інформаційних ризиків у системі інформаційно-комунікаційного забезпечення державно-управлінської діяльності. Особливої актуальності цей аспект діяльності інформаційно-аналітичного центру набуває в безпрецедентній кризовій ситуації в країні, що триває з 24 лютого 2022 р. через початок відкритого воєнного нападу рф на Україну.

Особливості діяльності управлінських структур в умовах відкритої воєнної агресії рф зумовлені наявністю багатьох факторів, що впливають на ефективність діяльності організацій, вимагають для прийняття результативних управлінських рішень: наявності великої кількості оперативної і достовірної інформації; регулярного проведення аналізу ретроспективи, чинного стану та можливих ситуацій; вибору варіанта управлінського рішення; організації виконання рішення та контролю як безпосередньо результатів, так і процесу його виконання.

Важливим аспектом, що впливає на рівень прийняття ефективних управлінських рішень в умовах відкритої воєнної агресії рф є наявність величезної кіль-