ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ЗДІЙСНЕННЯ ВІЙСЬКОВИХ ОПЕРАЦІЙ ТА БОЙОВИХ ДІЙ

PROBLEMS OF INFORMATION SECURITY DURING MILITARY OPERATIONS AND HOSTILITIES

УДК 305.08:417.011
DOI https://doi.org/10.32843/pma2663-5240-2022.28.35

Пархоменко-Куцевіл О.І.
д. наук з держ. упр., професор, завідувач кафедри публічного управління та адміністрування Університет Григорія Сковороди в Переяславі

У статті обґрунтовано важливість розповсюдження об'єктивної інформації у період проведення бойових дій та військових конфліктів, оскільки інформація – потужний інструмент та механізм маніпулювання будь-якими подіями, наслідками подій, суспільною думкою, формувати та впливати на певну оцінку подій тощо. Обґрунтовано, що інформаційна безпека відіграє ключову роль саме в періоди ведення військових дій та конфліктів. Адже неправильно, неправдиво подана інформація може спричинити панічні настрої у населення, впливати на хід подій, сприяти внутрішньому переміщенню населення, погіршенню іміджу політичного керівництва, породжувати недовіру до політиків, їх заяв, звернень, що може негативно впливати на ведення бойових дій, сприяє порушенню психічного та фізичного здоров'я населення, а також може нанести непоправної шкоди для всього результату військових дій. Тому запобігання розповсюдженню такої викривленої інформації в період військових конфліктів має важливе значення для всього перебігу військового конфлікту. Автором зазначено, що розповсюдження фейкових новин є однією з головних загроз на сьогодні інформаційній безпеці, адже не всі громадяни мають можливість отримувати правдиві новини або не всі громадяни знаходяться там, де відбуваються ці події, і отримують інформацію через ЗМІ, з Інтернет-ресурсів, від знайомих, родичів та ін. В період розгортання військових дій та конфліктів з'являється безліч фейкових новин про події в різних регіонах, дії влади щодо певних подій, думку та офіційні заяви, які суттєво можуть вплинути на результат військового конфліктів, війни. Запропоновані механізми протидії неправдивої, викривленої, непровіреної інформації в умовах військових конфліктів та бойових дій. По-перше, це формування медіаграмотності населення. По-друге, постійне висвітлення об'єктивної інформації через урядові інтернет-видання, ЗМІ, спілкування з громадянами. По-третє, встановлення відповідальності за фейки та розповсюдження їх серед населення. По-четверте, контроль фейкових акаунтів, які пересилають свідомо неправдиву, викривлену інформацію. По-п'яте, формування спеціальних підрозділів у кіберполіції, які займатимуть виявленням фейків, дипфейків та їх нейтралізації.

Ключові слова: *державне управління, інформація, інформаційна безпека, фейки, фейкові новини, військові дії, військові конфлікти.*

The article substantiates the importance of disseminating objective information during hostilities and military conflicts, as information is a powerful tool and mechanism for manipulating any events, consequences, public opinion, to form and influence a certain assessment of events, etc. The author substantiates that information security plays a key role in periods of hostilities and conflicts. After all, incorrectly, incorrectly presented information can cause panic in the population, affect the course of events, promote internal displacement, deteriorate the image of political leadership, create distrust of politicians, their statements, appeals, which can negatively affect hostilities, contributes to mental disorders and physical health of the population, and can cause irreparable damage to the entire outcome of hostilities. Therefore, preventing the dissemination of such distorted information during military conflicts is important for the entire course of a military conflict. The author argues that the spread of fake news is one of the main threats to information security today, because not all citizens have the opportunity to receive true news or not all citizens are where these events take place, and receive information through the media, Internet resources, from acquaintances, relatives, etc. During the period of hostilities and conflicts, there is a lot of fake news about events in different regions, government actions on certain events, opinions and official statements that can significantly affect the outcome of military conflicts, war. The article proposes mechanisms for disseminating and counteracting false, distorted, unverified information in the context of military conflicts and hostilities. The first is the formation of media literacy of the population. Secondly, the constant coverage of objective information through government online publications, the media, communication with citizens. Third, establishing responsibility for fakes and spreading them among the population. Fourth, control of fake accounts that send knowingly false, distorted information. Fifth, the formation of special units in the cyber police, which will deal with the detection of fakes, dipfeys and their neutralization.

Key words: *public administration, information, information security, fakes, fake news, military actions, military conflicts.*

Постановка питання. На сьогодні інформація є не тільки можливістю передачі знань, подій, описати емоції або почуття, це потужна зброя, яка може не лише маніпулювати свідомістю, а й вбивати, адже за допомогою інформації можна зробити певні нації, думки, ментальність – ворожою, сформувати негативне та вороже ставлення до подій, особистостей, особистих думок тощо.

Саме в період військової агресії Російської Федерації у 2022 році та війни з Україною, інформація набуває важливого та смертельного значення.

Інформація – це надсильний інструмент та механізм маніпулювання будь-якими подіями, наслідками подій, суспільною думкою, формувати та впливати на певну оцінку подій тощо.

Тому виникла нагальна проблема системного аналізу проблем забезпечення інформаційної безпеки України саме в умовах військових конфліктів та війни.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки, запобіганню викривленої інформації аналізують С. Горова, В. Горовий, М. Гуцалюк, С. Дацюк, В. Дереко, О. Довгань, Б. Кормич, В. Лужецький, В. Марков, О. Онищенко, В. Остроухов, О. Панченко, В. Петрик, О. Тихомиров, Я. Чмир, В. Шатун та інші. Перелічені вчені аналізують поняття «інформаційна безпека», основні загрози інформаційній безпеці, етапи забезпечення інформаційної безпеки, нормативно-правове забезпечення інформаційної безпеки України, визначення механізмів запобігання та протидії інформаційній безпеці та ін.

Існують поодинокі дослідження проблем розповсюдження фейків, фейк-новин. Так, О. Саприкін аналізує фейки як інструмент інформаційної війни проти України [1]. О. Курбан В. здійснює теоретичний аналіз ідентифікації та нейтралізації фейків у сучасних медіа [2].

Виділення невирішених раніше частин загальної проблеми. Однак, на сьогодні відсутні системні дослідження проблем забезпечення інформаційної безпеки в умовах військових конфліктів, обґрунтування механізмів забезпечення інформаційної безпеки в умовах військових конфліктів.

Мета статті є системний аналіз проблем забезпечення інформаційної безпеки України саме в умовах військових конфліктів та війни, визначення механізмів протидії неправдивої, викривленої, непровіреної інформації в умовах військових конфліктів та бойових дій.

Виклад матеріалу. Невипадково сучасне XXI століття у науковій літературі називають інформаційним. Масштабні трансформації соціуму, спричинені ґенезою нових форм соціальної організації, закономірно наводять до певних перенапруг інституційної системи, оскільки стабільна реальність починає заміщатися високо динамічною реальністю.

На сьогодні можемо констатувати, що інформаційна безпека зараз виходить на перший план. Після вторгнення Російської Федерації на територію України, віроломного знищення мирних міст та мирних жителів, жінок, дітей, ненадання можливості щодо евакуації мирних жителів, ми бачимо як російські засоби масової інформації маніпулюють інформацією, висвітлюють спаплюжену інформацію про начебто «військову операцію», маніпулюють інформацією щодо загиблих військовослужбовців та мирних жителів, а також постійно виправдовують свої дії та наполягають на небезпеці, яка йде від України. Таким чином, завдяки ЗМІ російська влада демонструє неважливість «військової операції» Росії, перемогу російської армії та незламність власної країни та влади.

Тому виникла загроза того, щоб блокування правдивої інформації, формування панічних настроїв, формування негативного сприйняття населенням ролі української армії, політичної еліти, дій державної влади має негативний вплив на розвиток ситуації та досягнення перемоги у цій війні.

Коротко можна сказати, що інформаційна безпека є неможливістю заподіяння шкоди властивостям об'єкта безпеки, які обумовлені інформацією та інформаційною інфраструктурою. Інформаційна безпека включає: стан захищеності інформаційного простору, завдяки якому забезпечується його формування та розвиток на користь держави, громадян та організацій; стан інформації, що виключає або порушує такі її властивості, як цілісність, конфіденційність та доступність; стан інфраструктури, що дозволяє використовувати інформацію строго за призначенням та без негативного впливу на систему; економічну складову, що містить телекомунікаційні та інформаційні системи та структури управління, такі як системи збору, акумуляції та обробки даних, загальноекономічного аналізу та прогнозування господарського розвитку, управління, координування та прийняття рішень; фінансову складову, що охоплює інформаційні мережі та бази даних, системи фінансових розрахунків та обміну [3].

Останніми роками відбувається насичення соціальної системи інформаційними потоками. Раніше подібних явищ в історії людства не було – як наслідок, практично немає наукового емпіричного та соціально-управлінського досвіду реагування на такі потоки.

Стрімке зростання соціальної значущості інформаційних технологій полягає в тому, що, як вважають дослідники, «соціальні мережі, месенджери, інтернет-магазини, онлайн-банкінг – всі ці засоби зв'язку та комунікації потенційно вразливі» [4].

Інформаційна безпека відіграє ключову роль саме в періоди ведення військових дій та конфліктів. Адже неправильно, неправдиво подана інформація може спричинити панічні настрої у населення, впливати на хід подій, сприяти внутрішньому переміщенню населення, погіршенню іміджу політичного керівництва, породжувати недовіру до політиків, їх заяв, звернень, що може негативно впливати

на ведення бойових дій, сприяє порушенню психічного та фізичного здоров'я населення, а також може нанести непоправної шкоди для всього результату військових дій. Тому запобігання розповсюдженню такої викривленої інформації в період військових конфліктів має важливе значення для всього перебігу військового конфлікту.

На сьогодні головними шляхами розповсюдження інформаційних викривлень та отримання недостовірної інформації (фейк), особливо в умовах військових конфліктів та війн, є: по-перше, надання інформації через соціальні мережі друзів або груп, на які підписані; надання інформації з підроблених акаунтів відомих людей, політиків, громадських діячів; надання інформації через огляд новин на телерадіомовних каналах; надання інформації через особисті повідомлення або у спільних групах Viber, Telegram, інші меседжери.

В аспекті забезпечення інформаційної безпеки особливе місце займає проблема поширення чуток – недостовірних повідомлень, що приймають різноманітні комунікативні форми, у тому числі. При цьому чутки, найдавніша форма соціальної комунікації, незважаючи на технологічний прогрес, поява Інтернету та телекомунікаційних технологій, не втратили свого впливу в системі комунікації, більш того, вони стали "віртуальними".

У зв'язку з цим слід зазначити, що висока швидкість передачі повідомлень у мережі, принципова анонімність інтернет-комунікації виявилися сприятливим середовищем для функціонування чуток. Порівняно з традиційними формами чуток, інтернет-чутки передаються з високою швидкістю та охоплюють за короткий термін величезну аудиторію, впливаючи на свідомість та поведінку людей [5]. Таким чином, науково-технологічний прогрес не тільки не викорінив цю давню форму соціальної комунікації, а також, навпаки, привів до її своєрідного оновлення та оновленої форми. Це один із парадоксів сучасної комунікаційної системи, ефективне рішення якого може сприяти оптимізації функціонування інституту держави.

На даний час, чутки не втратили свого значення і, на відміну від традиційних ЗМІ, не знижують свого впливу з появою Інтернету. Чутки адаптуються до нових умов та інтегруються у глобальну мережу, набуваючи нових, раніше не відомих властивостей. Так, значно збільшуються швидкість їх поширення та охоплення аудиторії.

Окремо стоїть проблема поширення фейків. Фейк – це подання фактів у спотвореному вигляді або подання свідомо неправдивої інформації. До того ж фейк – це спосіб маніпуляції свідомістю шляхом надання неповної інформації, спотворення контексту, частини інформації з метою підштовхнути аудиторію до дій чи думок, які потрібні маніпулятору [1; 2]. Як приклад фейків у сучасному інтернет-середовищі, можна навести багато неправдивої інформації щодо вакцинації від COVID-19, протікання хвороби, наслідки такої хвороби, поширення короновірусної інфекції у світі та регіону тощо.

Окремо стоїть розповсюдження фейкових новин, особливо це актуально в період військових дій, адже не всі громадяни мають можливість отримувати правдиві новини або не всі громадяни знаходяться там, де відбуваються ці події, і отримують інформацію через ЗМІ, з Інтернет-ресурсів, від знайомих, родичів та ін.

Фейкова інформація може приймати різні медіаформи – текст, фото, відео- або аудіо-повідомлення, звичайна та «вірусна» реклама в ЗМІ та соцмережах, вкидання в месенджерах Viber, WatsApp та ін., використання бот-мереж, що імітує гаряче обговорення живих співрозмовників на форумах та соціальних мережах. Для масованого просування фейкових новин діють ботоферми та «фабрики мережевих тролів». Широко практикується пранкінг, інші технологічні форми дезінформування, просування особистостей, теорій, ідей, проектів, партій – з метою створення у свідомості громадян певного бажаного їхнього образу (позитивного чи негативного).

В результаті в українському сегменті Інтернету панує багато викривленої, неправдивої, неперевіреної інформації, яка спотворює об'єктивну реальність, сучасні події, висловлення, заяви офіційних осіб, а також позиції посадовців. Описана системна проблема, яка не знаходить протягом тривалого часу свого рішення, створила передумови для погіршення якості інформації в медіапросторі сучасного соціуму. Стає очевидним, що в даний час у комунікаційній системі суспільства склалася складна ситуація, а якість інформації та актуальні ризики не дозволяють розмірковувати про інформаційної захищеності – як держави загалом, і масової аудиторії, і навіть індивідуальних споживачів інформації – у фізичній чи віртуальній реальності.

В інформаційній безпеці мають бути чітко позначені дві її складові аспекту:

інформаційно-технічний – захист, контроль та дотримання законності та правопорядку телекомунікаційній сфері (захист від: несанкціонованого доступу, хакерських зламів комп'ютерних мереж та сайтів, логічних бомб, комп'ютерних вірусів та шкідливих програм, несанкціонованого використання частот, радіоелектронних атак та ін.);

інформаційно-психологічний захист психіки суспільства та держави від негативного інформаційного впливу.

І саме інформація в ситуації військових дій стає додатковою зброєю ворога з урахуванням інформаційно-психологічного аспекту інформаційної безпеки.

В основу концепції захисту від психологічних наслідків інформаційної безпеки має лягти принцип інформації про стратегічний ресурс, а концепція виходити з наступних постулатів: свобода слова, незалежність ЗМІ та свобода друку основа громадянського суспільства; ЗМІ мають працювати на благо свого суспільства та держави; органам державної влади слід звертати увагу населення та ЗМІ на якість поданої інформації а також відповідальність за надання свідомо неправдивої та викривленої інформації.

Крім того, важливим аспектом інформаційно-психологічної безпеки є захист від прихованого інформаційного впливу, особливо це актуально для територій, де ведуться активні бойові дії. Науковці виділяють два основні методи прихованого інформаційного впливу: введення інформації в неусвідомлювані зони пам'яті, використовуючи навіювання, роз'яснення, навчання у дисоційованому стані тощо; забезпечення прямого доступу в пам'ять шляхом зміни стану свідомості, або навіть його відключення.

В період розгортання військових дій та конфліктів з'являється безліч фейкових новин про події в різних регіонах, дії влади щодо певних подій, думку та офіційні заяви, які суттєво можуть вплинути на результат військового конфліктів, війни.

Так, з'явилися засновані на технології штучного інтелекту генератори новин та синтезованого медіа-контенту, зокрема, фейкових новин, «глибоких фейків» (Deep Fake), що дозволяє робити реалістичні фото-, аудіо- та реалістичні відео-підробки (у тому числі, створені на основі лише голоси реальної особи). Так, дослідники з Технологічного університету Наньянга в Сінгапурі та китайські розробники штучного інтелекту SenseTime розробили метод створення «діп-фейків» на основі аудіозапису: штучний інтелект бере аудіозапис однієї людини, що з'єднує з фотозображенням або відео іншої людини (або тієї ж людини) – і генерує реалістичний відеозапис того, як людина вимовляє слова з джерела звуку; людина у відео стає маріонеткою для оригінального голоси [6]. В основі дип-фейків лежать генеративно-змагальні нейромережі, які в результаті навчання на реальному наборі аудіо-, відео- та фото-матеріали про певну персону можуть синтезувати реалістичний фейковий контент про цю персону, помістивши її в будь-яку роль, будь-який антураж, вклавши в мова, малюнок голосу та міміку будь-який текст. У глядача при перегляді дип-фейкового відео складеться враження, що він дивиться реально зняте відео.

Основними механізмами протидії неправдивої, викривленої, непровіреної інформації в умовах військових конфліктів та бойових дій є наступні.

По-перше, це формування медіаграмотності населення. Медіаграмотність виступає як комплексний феномен, що дозволяє населенню захищатися, в тому числі, від маніпулятивних впливів та брати участь у реалізації інформаційної безпеки. Медіаграмотність має чотири важливі складові – критичне мислення, медіа-орієнтування, медіа-споживання та медіа-дизайн [7]. Медіа-маніпуляція суспільною свідомістю чи думкою досягається за рахунок впливів на наше сприйняття через зір (це медіа-дизайн); через можливість орієнтуватися в інформаційних потоках, часто у рядового споживача їх дуже багато, а часу мало на фактичне орієнтування; через великі обсяги контенту, які сипляться на кожну людини, також через неможливість критично сприймати інформацію через довіру, наприклад, конкретним ЗМІ [7].

По-друге, постійне висвітлення об'єктивної інформації через урядові інтернет-видання, ЗМІ, спілкування з громадянами. Так, постійне надання інформації про важливі події, особливо у період проведення військових дій надасть можливість спростувати чутки та фейкові новини. Зокрема, на початку військового вторгнення Росії в Україну (24 лютого 2022 року) було запроваджено на всіх українських каналах інтерактивна програма «Інформаційний марафон», яка не лише висвітлювала об'єктивні події військового вторгнення, військових подій, пересування ворожої техніки, поразки та перемоги Збройних Сил України, а також висвітлювалися думки та надавалися коментарі посадових осіб, які перебувають в зоні бойових дій, постійно звертався до громадян Президент України, прем'єр-міністр України, міністри пояснюючи, що відбувається. Таким чином, зазначені дії надали державній владі уникнути фейків, фейкових новин та маніпуляцій щодо військових перемог та поразок, а також змінили відношення населення країни до керівництва держави, зменшили панічні настрої населення, покращити психологічне самопочуття населення, яке перебуває у зоні бойових дій.

По-третє, встановлення відповідальності за фейки та розповсюдження їх серед населення. Звичайно важливим елементом у забезпе-

ченні інформаційної безпеки як суспільства так і окремих громадян є встановлення відповідальності за надання свідомо недостовірної, непровіреної, викривленої інформації. Зокрема, це повинна бути кримінальна відповідальність, особливо коли така недостовірна інформація розповсюджується в період військових дій та конфліктів і наносить шкоду не тільки конкретному громадянину, а й суспільству в цілому.

По-четверте, контроль фейкових акаунтів, які пересилають свідомо неправдиву, викривлену інформацію. Наприклад, контроль за поширенням фейкової інформації впроваджують зараз великі месенджери. WhatsApp особливим символом позначає повідомлення, які занадто «далеко» пішли від свого автора, тобто пересилалися багато разів, що є відмінною рисою фейку.

По-п'яте, формування спеціальних підрозділів у кіберполіції, які займатимуть виявленням фейків, дипфейків та їх нейтралізацією.

Висновки. У статті проаналізовані проблеми забезпечення інформаційної безпеки в епоху військових дій та конфліктів. Визначено, що інформаційна безпека відіграє ключову роль саме в періоди ведення військових дій та конфліктів. Адже неправильно, неправдиво подана інформація може спричинити панічні настрої у населення, впливати на хід подій, сприяти внутрішньому переміщенню населення, що може негативно впливати на ведення бойових дій, сприяє порушенню психічного та фізичного здоров'я населення, а також може нанести непоправної шкоди для всього результату військових дій. Обґрунтовано, що головними шляхами розповсюдження інформаційних викривлень та отримання недостовірної інформації (фейк) є: по-перше, надання інформації через соціальні мережі друзів або груп, на які підписані; надання інформації з підроблених акаунтів відомих людей, політиків, громадських діячів; надання інформації через огляд новин на телерадіомовних каналах; надання інформації через особисті повідомлення або у спільних групах Viber, Telegram, інші меседжери. Запропоновані механізми запобіганню та протидії неправдивої, викривленої, непровіреної інформації в умовах військових конфліктів та бойових дій.

У перспективи подальших досліджень передбачено здійснити аналіз закордонного досвіду запобіганню розповсюдженню фейкових новин в умовах інформаційних війн та висвітлення військових подій.

ЛІТЕРАТУРА:

1. Саприкін О. А. Фейк як інструмент інформаційної війни проти України. *Бібліотекознавство. Документознавство. Інформологія*. 2016. № 1. С. 87-94.

2. Курбан О В. Фейки у сучасних медіа: ідентифікація та нейтралізація. *Бібліотекознавство. Документознавство. Інформологія*. 2018. № 3. С. 96-103. URL: http://nbuv.gov.ua/UJRN/bdi_2018_3_15

3. Грачева Е.А. Информационная безопасность. *The Newman in Foreign Policy*. 2020. Т. 3, № 54 (98). С. 57-59.

4. Грошева Е.К., Невмержицкий П.И. Информационная безопасность: современные реалии. *Бизнес-образование в экономике знаний*. 2017. № 3. С. 35-38.

5. Власенко М.С. Обеспечение информационной безопасности несовершеннолетних в сети Интернет: современное состояние и совершенствование правового регулирования. *Вестник Волжского университета им. В.Н. Татищева*. 2019. № 3. С. 98-105.

6. Cole Samantha, New Deepfake Method Can Put Words In Anyone's Mouth. *Tech by VICE* 24.01.2020. URL: https://www.vice.com/en_us/article/g5xvk7/researchers-created-a-way-to-makerealistic-deepfakes-from-audio-clips

7. Bykov I. A., Balakhonskaya L. V., Gladchenko I. A., Balakhonsky V. V. Verbal aggression as a communication strategy in digital society. *Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop*. Saint-Petersburg, 2018. P. 12–14.