ПУБЛІЧНЕ УПРАВЛІННЯ

DOI https://doi.org/10.58442/2522-9931-2024-27(56)-105-125
УДК [659.3:004] : 323.266 (477)

Кузьменкова Катерина Сергіївна,
Головний консультант відділу забезпечення
діяльності членів Комісії
Секретаріату Центральної виборчої Комісії, м. Київ;
аспірантка кафедри публічного управління і проектного менеджменту
Навчально-наукового інституту менеджменту та психології
ДЗВО «Університет менеджменту освіти».
Київ, Україна.
https://orcid.org/0009-0004-7107-8793
20000lpv@gmail.com

ДОСВІД СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ ЩОДО ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА МОЖЛИВОСТІ ЙОГО ВИКОРИСТАННЯ В УКРАЇНІ

Анотація. У статті здійснено аналіз досвіду протидії дезінформації на основі функціонування основних суб'єктів кіберпростору США. Визначено позитивні риси США що стосуються протидії дезінформації, а саме: усвідомлене і чітко сформоване розуміння масштабу проблеми дезінформації; співпраця між різними секторами щодо протидії дезінформації; ефективна цифрова освіта громадян, перевірка фактів і стеження за дезінформацією; наявність дієвих інструментів та технологій, що сприяють посиленню кіберзахисту. Здійснено аналіз діяльності американських урядових інституцій та агенцій у сфері забезпечення кібербезпеки. Вказано, що одним із ключових аспектів досвіду Америки у протидії дезінформації є активна роль уряду щодо виявлення, аналізу та відвернення дезінформації. Акцентовано на тому, що США володіють величезним фінансовим, технологічним, науково-технічним і військовим потенціалом, а також приділяють значну увагу зміцненню національної безпеки, захисту прав громадян і комерційних інтересів в інформаційній сфері. Зазначено, що загальносуспільним завданням для США, яке потребує спільних зусиль є агресивна політика росії та посилення російської дезінформації та пропаганди. Визначено можливості використання зазначеного досвіду США в Україні в таких напрямах, як: забезпечення прозорості в діяльності медіа, посилення міжнародної співпраці у сфері кібербезпеки, зміцнення критичного мислення у громадян та формування медіастійкості особливо в

https://doi.org/10.58442/2522-9931-2024-27(56)

умовах російської інтервенції, створення та забезпечення ефективного функціонування на кшталт Агентства (Центру) протидії дезінформації, прийняття технологічних рішень з метою виявлення та відсторонення дезінформаційних впливів, регулювання соціальних мереж та платформ, які поширюють фейки, чутки і дезінформацію, становлення та розвиток вітчизняної системи законодавства, що стосується боротьби з дезінформацією тощо. Доведено, що боротьба з дезінформацією має сприяти зміцненню демократії, свободи слова та інформаційної безпеки, а досвід США у сфері управління інформацією та технологіями боротьби з дезінформацією є актуальним в умовах сьогодення для України.

Ключові слова: дезінформація; зарубіжний досвід протидії дезінформації; фейк; кібертероризм; кібербезпека; кіберпростір.

ВСТУП / INTRODUCTION

Постановка проблеми. У сучасному цифровому світі питання поширення дезінформації та фейків стають все більш актуальними і це викликає серйозну загрозу для демократичних процесів і громадської довіри. Досвід США, щодо протидії цим явищам може стати цінним джерелом навчання і надихнути інші країни, включаючи Україну, розробляти власні стратегії боротьби з дезінформацією. Дезінформація і фейк-новини стали серйозними світовими проблемами, завдавши значної шкоди довірі до медіа та громадянському суспільству. Спроби впливати на громадську думку через маніпуляції інформацією стають все більш виразними і складними завдяки розвитку технологій та соціальних мереж. США, як світовий лідер, зіткнулася з цими викликами і в досвіді цієї країни є багато цінних уроків для держав інших країн, включаючи Україну.

Аналіз останніх досліджень та публікацій. У науковій літературі існує досить ґрунтовна джерельна база, що стосується дослідження вказаної наукової тематики. Окремі аспекти дослідження: дезінформації, впливу фейків на суспільну свідомість; формування кіберпростору; фундаментальних засад кібербезпеки; підготовки кваліфікованих кадрів для органів публічної влади з відповідною кіберосвітою; кращих практик зарубіжного досвіду у сфері боротьби з дезінформацією присвячено праці таких науковців, як: Л. Арсеновича [6], Б. Андрушківа, О. Гагалюк, Н. Кирич, О Погайдак [4], О. Євсюкової [5], О. Звоздетської [1], В. Маляренко [3] Т. Павленко [2] тощо. Проте останні здобутки кращих зарубіжних практик у площині деталізації, саме, американського досвіду боротьби з дезінформацією не охоплюють всі аспекти дослідження, оскільки реалії

https://doi.org/10.58442/2522-9931-2024-27(56)

сучасного цифрового світу і зокрема, України, створюють нові обставини для його вивчення і використання.

МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Мета статті полягає у теоретичному аналізі зарубіжного досвіду протидії дезінформації на прикладі такої країни, як США та визначенні можливостей (напрямів) щодо його використання в Україні.

Відповідно до зазначеної мети у статті поставлено такі ***завдання***: охарактеризувати функціонування основних суб'єктів кіберпростору США; здійснити аналіз позитивних рис, що стосуються протидії дезінформації у США; визначити можливості використання зазначеного досвіду США в Україні.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ / THE THEORETICAL BACKGROUNDS

Зазначимо, що серед науковців, які займаються проблематикою щодо визначення поняття, впливу та наслідків дезінформації є О. Звоздетська. Вітчизняна дослідниця розглядає дезінформацію як загрозу національній безпеці Європейського Союзу, досліджує підходи до визначення та розуміння комплексної проблеми забруднення інформаційного простору неправдивою інформацією. Цілком доцільно авторка зазначає, що вказана загроза підриває не лише інформаційну безпеку європейських країн, а й загрожує основним нормам та демократичним цінностям, від яких залежить інституційна легітимність та політична стабільність Європейського Союзу. У цих умовах, на думку дослідниці, важливо забезпечити об'єктивне та засноване на доказах розуміння змісту, масштабу, обсягу, характеру існуючої проблеми, а також розробити можливі відповіді, які враховуватимуть що, проблема дезінформації глибоко переплетена з цифровою екосистемою, технологіями, які постійно розвиваються та вдосконалюються. Відтак варто погодитися з О. Звоздецькою, що проблемою, яка утруднює вивчення феномену «дезінформації», є наявність чисельної термінології, яка позначає неправдиву інформацію, зокрема фейки, дезінформація, пропаганда, маніпулювання інформацією, інформаційний розлад, гібридна війна. Неузгодженість дефініцій вказує на відсутність консенсусу серед ключових зацікавлених сторін щодо сфери розуміння питання [1].

Інша українська дослідниця Т. Павленко у власних наукових працях торкається таких аспектів, як аналіз змісту поняття «дезінформація» з урахуванням міжнародного досвіду такого визначення та складових

https://doi.org/10.58442/2522-9931-2024-27(56)

елементів дезінформації, а саме: різновиди, типи та зміст контенту, який створюється та передається; усвідомлення, мотиви та мета, якими послуговуються особи, що створюють/розповсюджують такий контент; способи розповсюдження контенту. Значної уваги Т. Павленко приділяє ознакам дезінформації та наслідкам її впливу. Наукову цікавість становить авторське розуміння дезінформації, як спотворену, свідомо неправдиву, провокаційно-тенденційну інформацію, з питань що становлять суспільний інтерес, що створюється, подається та/або поширюється як правдива з метою введення в оману громадськості, політичних опонентів, конкурентів тощо та/або спричинення серйозної суспільної шкоди. Також, дослідниця аргументує необхідність встановлення адміністративної та кримінальної відповідальності за дезінформацію, наголошуючи на тому, що дезінформація є однією з ключових загроз національній безпеці (основним її напрямам воєнній, державній, інформаційній та кібербезпеці, громадській безпеці) [2].

Дослідженню зарубіжного досвіду боротьби з фейками і дезінформації присвячені наукові праці ще одного з українських науковців – В. Маляренка. Автор розглядає зміст поняття «фейки» та визначає засади, способи виявлення фейків та дезінформації на прикладі країн ЄС, зазначаючи, що у світі існує два підходи до сфери відповідальності за поширення фейкової інформації. Перший (європейський) підхід передбачає цивільно-правове врегулювання відповідальності за дифамацію у медіа та відповідальність за поширення фейків. Другий – кримінальне переслідування за поширення такої деструктивної інформації як приватних осіб, так і медіа. Загальновідомим є той факт, що будь-яка, навіть позитивна фейкова інформація в результаті має негативний вплив та є загрозливим явищем у медіа просторі. Отже, дезінформація визначається різноманітними фейками, які поширюються державою-агресором з метою повалення конституційного ладу в Україні. В цілому, В. Маляренко узагальнює практику європейських держав щодо криміналізації поширення недостовірної інформації та фейків [3].

Представники когорти вітчизняних дослідників, які займаються даною науковою тематикою, а саме: Б. Андрушків, О. Гагалюк, Н. Кирич, О. Погайдак приділили значну увагу розумінню культ-освітнього компоненту у сфері управління, як засобу попередження вульгаризму у взаємовідносинах та поширенні фейків в медіа, опису важелів посилення економічної безпеки в державі. На переконання вказаних науковців, значну роль у розумінні проблематики дезінформаційних впливів відіграє етимологічний зміст таких понять, як: «вульгаризм», «плітки», «чутки», «фейки». За їх спільним переконанням, саме розв'язання проблеми

https://doi.org/10.58442/2522-9931-2024-27(56)

попередження вульгаризму, пліток, чуток і фейків, як одного з напрямів розвитку національної безпеки в умовах гібридної війни сприятиме не лише стабільності економіки, а й забезпечення спокою у суспільстві [4].

Обґрунтуванню актуальності осмислення кібербезпеки держави, як однієї з найважливіших галузей цифрового суспільства присвячено наукові праці вітчизняної дослідниці О. Євсюкової, яка визначає об'єктивну необхідність функціонування системи підготовки фахівців у сфері кібербезпеки, що, на думку авторки, обумовлено зростанням кіберзлочинності та кіберзагроз у сучасному світі. У даному контексті О. Євсюкова також досліджує досвід підготовки фахівців із кібербезпеки на базі навчальних закладів США, що мають світове визнання у цій сфері; акцентує увагу на питаннях стандартизації підготовки зі спеціальності 125 «Кібербезпека» та на фахових компетенціях фахівців у сфері кібербезпеки. Варто погодитися з думкою дослідниці, що підготовка висококваліфікованих кадрів з кібербезпеки для органів публічної влади залишається ключовим елементом повноцінної життєдіяльності держави. Для визначення, діагностики та дослідження проблем, які стосуються як діяльності органів публічної влади, так і осіб, що їх очолюють у сфері кібербезпеки, здатності передбачати проблеми, які стосуються життєдіяльності та безпеки держави, необхідні відповідна кваліфікація та вміння. Щодо останніх, то особливо необхідними є вміння: думати, аналізувати інформацію, приймати відповідні рішення та діяти, тобто реалізовувати рішення, які відповідають потребам та вимогам громадян за належне функціонування системи підготовки фахівців у сфері кібербезпеки формування обумовлене необхідністю її покращення, що є надзвичайно важливим для забезпечення довіри людей до інновацій, взаємозв'язку та автоматизації, отримання переваг від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації [5].

Серед когорти молодого покоління науковців, які займаються проблематикою кібербезпеки та кіберосвіти варто згадати Л. Арсеновича, який зосередив свою увагу на проблематиці професійного розвитку фахівців з кібербезпеки у публічному управлінні. Авторський проєкт професійного стандарту «Фахівець із кібербезпеки» є важливим щодо подальшого розвитку системи підготовки кадрів у сфері кібербезпеки, що не втрачає актуальності в умовах сьогодення [6].

Одним із ключових аспектів досвіду США в протидії дезінформації є активна роль уряду у виявленні, аналізі та відверненні дезінформації. Американські спецслужби та аналітичні центри займаються пошуком іноземних та внутрішніх дезінформаційних кампаній, а також надають публіці інформацію про виявлені загрози. Це допомагає підтримувати

https://doi.org/10.58442/2522-9931-2024-27(56)

відкритість та прозорість в інформаційному просторі. Другим важливим аспектом є співпраця між урядом, медіа та громадськими організаціями. У США існують програми та ініціативи, спрямовані на підвищення медіаосвіти серед населення, що допомагає громадянам розрізняти правдиву інформацію від фейків. Україна також має потенціал для розвитку подібних ініціатив та співпраці між різними секторами суспільства.

З огляду на те, що США не тільки володіють величезним фінансовим, технологічним, науково-технічним і військовим потенціалом, а й приділяють значної уваги зміцненню національної безпеки, захисту прав громадян і комерційних інтересів в інформаційній сфері, досвід цієї країни у сфері управління інформацією та технологій боротьби з дезінформацією є актуальним в умовах сьогодення.

У межах, передбачених універсальними документами по боротьбі з інформаційним тероризмом і відповідними міжнародними нормами в галузі прав людини, урядам країн надається значна ступінь гнучкості у виборі бажаних підходів, тому підходи до розв'язання проблеми розрізняються у кожній державі.

Так, серед основних антитерористичних актів США слід виділити: Акт про об'єднання і зміцнення Америки шляхом надання належних коштів, необхідних для перехоплення інформації та перешкоджання тероризму («Акт США про патріотизм 2001 р.» (USA PATRIOT ACT); Закон «Про надання додаткових повноважень спецслужбам в сфері боротьби з тероризмом» (2001 р.), Виконавчу директиву Президента США № 62 (1998) [7], [8].

Насамперед, варто охарактеризувати нормативно-правові засади, що стосуються боротьби з дезінформацією. Зокрема у розділі параграфу 3369 «Спільні дії з виявлення та протидії діяльності іноземного впливу» Розділу 50 «Війна і національна безпека» Кодексу США (The United States Code (formally the Code of Laws of the United States of America) вказано, що Конгрес визнав, росію, як державу, що веде інформаційну війну для досягнення своїх стратегічних інтересів за допомогою Центрального розвідувального управління (ЦРУ) разом зі своїми філіями (насамперед, російським агентством інтернет-досліджень), спрямовану проти США та їхніх союзників і партнерів. З огляду на таємне використання прокремлівською фракцією американських приватних онлайн-платформ соціальних мереж (Twitter, Facebook, Instagram, MySpace, LinkedIn та інші), Кодекс США (The United States Code (formally the Code of Laws of the United States of America) необхідне негайне застосування вимог до провайдерів, що стосуються видалення будь-якої дезінформації у повному обсязі [9].

https://doi.org/10.58442/2522-9931-2024-27(56)

З метою спостереження за розвитком таких ситуацій Національною розвідкою США, спільно з Міністерством оборони США було створено Центр аналізу загроз і даних у соціальних мережах (Social Media Data and Threat Analysis Center), який з червня 2021 р. є незалежною, неприбутковою організацією, що фінансується за рахунок грантів та комерційних контрактів.

У форі громадського контролю функціонує механізм звітування перед парламентом США. Наступним кроком для втілення американським законодавцем стане інтеграція повноважень і компетенцій вищезазначеного Центру (Social Media Data and Threat Analysis Center) в окремий Закон Палати представників парламенту США.

Виходячи з положень цього Закону, систематизуючи одинадцять основних завдань, основними сферами компетенції Центру (Social Media Data and Threat Analysis Center) є, по-перше, співпраця з компаніями соціальних медіа для проведення спільного аналізу інформаційних даних соціальних медіа, іноземного впливу, хакерських атак, витоків інформації, іншої незаконної діяльності та джерел фінансування, а по-друге, досить важливим є співпраця з незалежними експертами, неурядовими організаціями. Ключова роль Центру полягає в координації та взаємодії між третіми сторонами, такими як журналісти, федеральні центри впровадження досліджень, наукові кола, медіа та іноземні партнери [10].

Ще одним суттєвим виявом уваги американських держпосадовців стала ухвала 4 грудня 2014 р. Палатою представників Конгресу США Резолюції «Про рішуче засудження дій російської федерації під керівництвом в. путіна, якими було впроваджено політику агресії проти сусідніх країн з метою політичного та економічного домінування» у якій гостро засуджується російська федерація за проведення політичної агресії проти сусідніх країн з метою політичного та економічного домінування. В аргументаційній частині документу детально перелічуються основні аспекти агресивної політики росії щодо України, Грузії та Молдови; міжнародні договори, які зазнали порушень внаслідок цих дій (Статут ООН, Будапештський меморандум); дії, що підривають двосторонні відносини зі США (хакерські атаки на урядові мережі, порушення Договору про ліквідацію ракет середньої та малої дальності); а також встановлення шляхом фальсифікації виборів у росії авторитарного режиму під керівництвом в. путіна (переслідування політичних опонентів, ліквідація незалежних медіа, захоплення ключових секторів економіки) [11].

В ухваленій резолюції конгресмени закликали Президента США та Держдепартамент розробити стратегію виробництва і поширення новин та іншої інформації російською мовою в країнах зі значною часткою

https://doi.org/10.58442/2522-9931-2024-27(56)

російськомовного населення. Члени Палати представників Конгресу США рекомендували використовувати для поширення інформації вже існуючі платформи, такі як «Голос Америки» і «Свобода / Вільна Європа», сприяти створенню приватних компаній за участі держави для випуску відповідного контенту і залучити до реалізації цього завдання уряди країн регіону. Крім цього, 4 березня 2015 р. було ухвалено рішення про надання Наглядовою радою США з міжнародного мовлення (Broadcasting Board of Governors) 23,2 млн $ на програми російською мовою [12].

У березні 2016 р. до Сенату США було подано законопроект «Про протидію інформаційній війні» (Countering Information Warfare Act of 2016) яким передбачалася розробка комплексної стратегії протидії дезінформації та пропаганді, що поширюються росією та Китаєм по всьому світу [13].

Законопроект наголошував на необхідності координації дій з країнами-партнерами, особливо тими, проти яких проводяться дезінформаційні операції, а також з міжнародними організаціями та іншими органами, такими, як Європейський фонд за демократію (The European Endowment for Democracy) та Робоча група зі стратегічних комунікацій Європейської служби зовнішньополітичної діяльності (The European External Action Service Task Force on Strategic Communications) [14].

Зазначений нормативно-правовий документ передбачає створення Центру аналізу та реагування (Center for information analysis and response) який забезпечить:

- збір, обробку, інтеграцію та аналіз інформації, включаючи розвідувальні звіти, дані та аналітику від урядових установ США;
- обробку та поширення «фактологічних, описових та аналітичних контрпропагандистських матеріалів, що викривають дезінформацію, спрямовану проти США, їхніх союзників та партнерів»;
- виявлення поточних та нових тенденцій у сфері дезінформаційної пропаганди;
- зовнішню класифікацію країн і груп населення, найбільш вразливих до пропаганди та дезінформації.

У травні 2016 р. законопроект було внесено до Палати представників Конгресу США під назвою: «Про боротьбу з іноземною дезінформацією та пропагандою» Countering Foreign Propaganda and Disinformation Act [15].

У грудні 2016 р. положення вказаного законопроекту були імплементовані до Закону «Про національний оборонний бюджет» (National Defense Authorization) [16].

https://doi.org/10.58442/2522-9931-2024-27(56)

У результаті ухвалених положень у Державному департаменті США було створено Центр глобальної взаємодії (Global Engagement Center) [17].

У липні 2017 р. Конгрес США завершив процедуру голосування за новим законом, що посилює санкції відносно росії [18]. Одночасно, Офіс президента США, офіційно зазначив, що росія за допомогою модернізованої та деструктивної тактики втручається у внутрішні справи країн по всьому світу, проводить інформаційні операції в рамках агресивної кібер-кампанії з метою впливу на світову громадську думку. Кампанія впливу поєднує проведення таємних розвідувальних операцій, створення фейкових онлайн-персон державних медіа, сторонніх посередників, діяльність проплачених користувачів соціальних мереж і «тролів».

16 січня 2018 р. сенатори США Марко Рубіо та Кріс Ван Холлен (Marco Rubio, Chris Van Hollen) представили положення до Закону «Про національний оборонний бюджет» (National Defense Authorization) у якому мова йде про запровадження санкцій проти країн, які втручаються у виборчий процес США [19].

Зокрема, йдеться про використання соціальних і традиційних медіа для поширення неправдивої інформації, купівлю реклами, яка впливає на вибори, а також блокування або перешкоджання доступу до виборчої інфраструктури. Міністерство оборони США розпочало чергову кампанію з боротьби з іноземною пропагандою та дезінформацією в рамках нового партнерства з Пентагоном. Міністерство оборони США перерахувало 40 мільйонів доларів бюджетних коштів Центру глобальної взаємодії (далі – ЦГВ) для реалізації різних «ініціатив з протидії іноземній пропаганді та дезінформації». Згідно з повідомленням Держдепу, «організації громадянського суспільства, виробники інформації, неурядові організації, науково-дослідні центри, що фінансуються з федерального бюджету, приватні компанії та академічні установи мають право брати участь у конкурсі на отримання грантів від ЦГВ». Спочатку на гранти було виділено 5 мільйонів доларів США. Крім того, ЦГВ співпрацюватиме з Пентагоном над розробкою інших пілотних проєктів в боротьбі з дезінформацією [20].

У квітні 2018 р. екс-президент США Дональд Трамп провів саміт з лідерами Литви, Латвії та Естонії, на якому заявив, що США співпрацюватимуть з країнами Балтії для зміцнення довіри до інституцій цих країн у протидії дезінформації, шляхом зміцнення регіональних незалежних медіа, громадського мовлення та посилення медіаграмотності населення. Представники Республіканської та Демократичної партій США 2 серпня 2018 р. представили законопроект «Про національний оборонний бюджет» (National Defense Authorization), спрямований на посилення

https://doi.org/10.58442/2522-9931-2024-27(56)

санкцій і тиску на росію, що передбачав, зокрема, посилення санкцій проти енергетичного та фінансового секторів росії, а також запровадження цільових обмежень проти державних інституцій, олігархів та кібер-акторів. Крім того, у законопроекті йшлося про необхідність посилення боротьби з російською дезінформацією та пропагандою, а також про створення національного центру з реагування на російські загрози, який може передавати інформацію стейкхолдерам сектору безпеки з даними на предмет загроз відносно системи національної безпеки чи порушень чинного законодавства внаслідок діяльності зовнішніх акторів використовуючи соціальні мережі. Також, Центр повинен мати доступ до національних органів влади для розслідування та аналізу їхньої діяльності та право на створення архіву зведених даних про іноземні впливи та кампанії з метою вироблення спільного підходу до характеру загрози та сприяння проведенню професійних інформаційних кампаній, зі строгим дотриманням конфіденційності [21].

24 липня 2023 р. International Business Machines (далі – IBM) опублікувала звіт про вартість витоку даних за 2022 р., де зазначається про те, що середня вартість витоку даних у США досягла рекордного рівня в 4,45 мільйона доларів США, що на 2,3 % більше, ніж у 2022 р. У порівнянні з 2020 р. середня вартість зросла на 15,3 %. Загалом, 51 % організацій вирішили збільшити інвестиції в безпеку після витоку даних. Ключові сфери для додаткових інвестицій включають реагування на інциденти, навчання співробітників та технології виявлення/реагування на загрози.

AI/Automation cut breach lifecycles by 108 days; $ 470,000 in extra costs for ransomware victims that avoid law enforcement; Only one third-of organizations detected the breach themselves; (ШІ/Автоматизація скоротила життєвий цикл зламу на 108 днів; $ 470 000 додаткових витрат для жертв програм-вимагачів, які уникають правоохоронних органів; Лише третина організацій виявила злом самостійно) [22].

Атаки зловмисників спричинили найбільший середній збиток – 4,9 млн доларів США, що на 9,6 % більше, ніж у середньому. Фішинг (англ. *phishing*) – це відносно новий вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів, мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переведення або обміну, валюти, інтернет-магазинів. Шахраї використовують усілякі прийоми, які найчастіше змушують користувачів особисто повідомити конфіденційні дані (наприклад, шляхом надсилання електронних листів із пропозиціями підтвердити реєстрацію аккаунта, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

https://doi.org/10.58442/2522-9931-2024-27(56)

Викрадені облікові дані (328 днів на виявлення) та зловмисні дії інсайдерів (308 днів) були найдовше виявлені та локалізовані. Фішингові атаки виявляли в середньому за 293 дні.

На основі висновків цього звіту IBM варто окреслити заходи, які необхідно впроваджувати, щоб, зменшити вплив та витрати від витоку даних:

1) розробка та розгортання безпечного програмного забезпечення;
2) системне використання методології DevSecOps (безпека операцій) та безперервного тестування;
3) модернізація захисту даних у гібридних хмарних середовищах;
4) посилення контролю конфіденційних даних, розподілених між декількома хмарами;
5) використання штучного інтелекту, для підвищення швидкості і точності безпекових операцій;
6) впровадження цифрових інструментів у робочі процеси виявлення, реагування та розслідування;
7) формування чіткого уявлення про зону ризику для організації та державних установ та посилення більш ефективного реагування на інциденти;
8) визначення пріоритетів на основі реальних ризиків та їх моделювання

Варто також зазначити про функціонування Центру ФБР зі збору скарг на злочини в Інтернеті (IC3) англ. Internet Crime Complaint Center) (надалі – IC3). Вказаний підрозділ, забезпечує систематизацію обробки повідомлень про злочини в Інтернеті, які надходять від громадських інституцій. Зокрема, CyWatch – це оперативний центр ФБР, який працює цілодобово, відстежуючи інциденти та підтримуючи зв'язок зі своїми місцевими відділеннями в США 24 години на добу, 7 днів на тиждень. Підтримка у боротьбі з кіберзлочинністю та дезінформацією IC3 здійснюється з приватним сектором і місцевими, державними, федеральними та міжнародними установами: створює можливість щодо використання порталу для постраждалих від кібертероризму та для повідомлень про інтернет-злочини (www.ic3.gov); забезпечує надання центрального вузла для публічних оповіщень; допомагає у в проведенні інформаційної діагностики, надання скарг і заморожування активів; розміщує базу даних віддаленого доступу для всіх правоохоронних органів через веб-сайт ФБР LEEP (The Law Enforcement Enterprise Portal). Загалом у США щонайменше двадцять федеральних департаментів та агенцій мають у складі штатних експертів по боротьбі з кіберзлочинністю та дезінформацією. Найбільш відкритим для спілкування з пресою є

https://doi.org/10.58442/2522-9931-2024-27(56)

Агентство з кібербезпеки та безпеки інфраструктури при Міністерстві національної безпеки США (CISA, Cybersecurity and Infrastructure Security Agency), яке активно залучає громадськість до співпраці. Відділ ФБР із кіберзлочинності публікує цінну статистику, за допомогою якої можна доповнити статті об'єктивними фактами про кібератаки та збитки від них. Серед інших джерел – Секретна служба США й Міністерство фінансів США. Допомогу можна також отримати від аналогічних державних установ інших країн світу [22].

Враховуючи вищезазначене, доцільно визнати, що боротьба з кіберзлочинністю має стати важливим напрямом співпраці України з Америкою. З цією метою у 2021 р. делегація Державної служби спеціального зв'язку та захисту інформації України та представники Офісу кібербезпеки та інфраструктурної безпеки Державного департаменту США домовилися про співпрацю. Також, у 2021 р. міністри оборони України та США підписали Рамкову угоду про Стратегічні рамки оборонного партнерства. Ця угода дозволяє розвивати співпрацю у сферах кіберзахисту, розвитку кіберпотужності та захисту критичної інформаційної інфраструктури. Зокрема, вона включає співпрацю у сфері кіберзахисту для стримування зловмисної кібердіяльності у системах національної безпеки, розвиток потенціалу та співпрацю у боротьбі з дезінформацією.

МЕТОДИ ДОСЛІДЖЕННЯ / RESEARCH METHODS

Методологічною основою статті є сукупність як загальнонаукових, так і спеціальних методів наукового пізнання, емпіричного і теоретичного рівнів дослідження, які застосовувались на різних етапах, зокрема загальнонаукового аналізу (у процесі аналізу наукових джерел та державних документів, що стосуються боротьби з кіберзлочинністю та функціонування державних інституцій у цій сфері); систематизації та узагальнення інформаційних даних; порівняльного аналізу здобутих даних (при виявленні переваг використання протидії дезінформації; метод контент-аналізу для дослідження системи законодавства та нормативно-правових актів, що регулюють діяльність урядових інституцій в США, що забезпечують подолання кіберзлочинності; методи дедукції, індукції та аналітичний метод застосовано під час узагальнення й аналізу емпіричної інформації за тематикою статті.

https://doi.org/10.58442/2522-9931-2024-27(56)

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESULTS OF THE RESEARCH

Відтак, узагальнено позитивні риси досвіду США для України, серед яких:

1. Усвідомлене і чітко сформоване розуміння масштабу проблеми:

Перше, що потрібно зробити – це ретельно вивчити та зрозуміти масштаби проблеми дезінформації в Україні. Це означає аналізувати джерела дезінформації, їх призначення та наслідки для українського суспільства.

2. Співпраця між різними секторами.

У США протидія дезінформації є завданням не тільки урядових органів, а й громадських організацій їх лідерів та активістів, медіа. Щодо України то варто акцентувати увагу на налагодженні плідної співпраці між всіма суб'єктами системи публічного управління для посилення ефективної боротьби з кіберзлочинністю.

3. Ефективна цифрова освіта громадян.

Розуміння принципів критичного мислення та медіаграмотності є ключовим для запобігання поширенню дезінформації як в американському так і українському суспільствах. Програми з медіаграмотності мають бути впроваджені в освітній процес і підтримуватися громадськими ініціативами.

4. Перевірка фактів і стеження за дезінформацією.

Спеціалізовані організації і фактчекери в США відіграють важливу роль у виявленні та спростуванні дезінформації. Варто відзначити, що і в Україні вже існують подібні ініціативи.

5. Посилення кіберзахисту.

Забезпечення кіберзахисту та безпеки інформації є важливим аспектом в боротьбі з дезінформацією в США. Україна повинна більш інтенсивно інвестувати у кіберзахист та реагування на кіберзагрози. Особливої актуальності це набуває за умов сьогодення, особливо в умовах збройної агресії росії на території української держави.

Отже, досвід США може слугувати джерелом навчання для України та інших країн у боротьбі з дезінформацією. Важливо розглядати цю проблему як загальносуспільне завдання, що потребує спільних зусиль усіх секторів суспільства. Боротьба з дезінформацією має сприяти зміцненню демократії, свободи слова та інформаційної безпеки.

Україна, яка вже досить тривалий час перебуває у стані інформаційної війни та здійснює боротьбу з агресію росії, має активно використовувати досвід США в протидії дезінформації. Важливо розвивати медіаосвіту серед громадян, сприяти співпраці з медіа, громадськими організаціями та урядом, а також встановлювати ефективні механізми

https://doi.org/10.58442/2522-9931-2024-27(56)

регулювання інформаційної безпеки в Інтернеті. Завдяки цим заходам, Україна може збільшити свою стійкість до дезінформації та зміцнити демократичні процеси в країні. Досвід США слугує важливим джерелом навчання, яке може бути використано для досягнення вказаних завдань.

Аналізуючи досвід США у боротьбі з дезінформацією в українській державі, на нашу думку, є необхідність щодо створення спеціальної інституції (або трансформації діяльності вже існуючого Центру протидії кіберзлочинності) на прикладі функціонування Центру надання скарг про кіберзлочини (ІС3) у США. Актуалізація створення такого центру (з відповідним веб-сайтом) полягає в тому, що повідомлення про кіберзлочини відбуватиметься на спеціально створеній інтернет-платформі, яка забезпечить єдиний підхід до аналізу та оцінювання отриманої інформації, а також надаватиме органам державної влади, органам місцевого самоврядування, бізнесу інформацію про поточну ситуацію, потенційні та можливі кіберзагрози, кібератаки та кіберзлочини, а також консультації представникам органів публічної влади, компаніям та громадськості щодо того, як захиститися від таких загроз, атак та злочинів; забезпечить «гібридний» підхід, що передбачає залучення експертів з традиційними навичками та знаннями у сфері кримінальних розслідувань та експертів зі спеціалізованими навичками та знаннями у сфері високих технологій. В умовах воєнного стану необхідно перейняти досвід США щодо створення «гібридних» підрозділів з розслідування кіберзлочинів, які об’єднують експертів зі спеціалізованими високотехнологічними навичками та знаннями. Зокрема, така співпраця може покращити збір та аналіз інформації про кіберзагрози, розробляти та використовувати інструменти для протидії кібератакам, а також підвищити рівень обізнаності усіх суб’єктів системи публічного управління (органів влади, бізнес-структур та громадських організацій) про кіберзагрози та способи протидії їм, що є важливим для належного функціонування не тільки національної економіки, але й держави в цілому.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ / CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

Поряд з численними іншими країнами, США сьогодні системно вирішують проблематику, що стосується боротьби з дезінформації і запобіганню спроб втручання у власні внутрішні державні справи за допомогою інформаційних маніпуляцій. Проте, США має великий досвіду у боротьбі з вказаними загрозами.

https://doi.org/10.58442/2522-9931-2024-27(56)

Можливості використання досвіду США, на нашу думку, в Україні включають наступне:

1. Створення Агентства протидії дезінформації. Україна може розглянути можливість створення спеціалізованого агентства, яке б координувало заходи протидії дезінформації та розробляло стратегії для виявлення та відповіді на фейки.

2. Зміцнення критичного мислення у громадян України. Американські програми та ініціативи з підвищення медіаграмотності можуть бути адаптовані для українського суспільства, допомагаючи громадянам краще розуміти, аналізувати та відрізняти правдиву інформацію від дезінформації.

3. Посилення міжнародної співпраці у сфері кібербезпеки. Україна може співпрацювати з американськими та іншими партнерами для обміну досвідом, ресурсами у сфері боротьби з дезінформацією та кіберзагрозами.

4. Забезпечення прозорості у медіа. Створення та підтримання прозорих та незалежних медіа може допомогти знизити вплив дезінформації. Моделі, які функціонують у США, можуть слугувати прикладом для розвитку українських медіаорганізацій.

5. Розвиток кіберзахисту та забезпечення безпеки інформаційних систем є ключовими аспектами у боротьбі з дезінформацією. Україна може використовувати досвід США у цій сфері для захисту своєї інформаційної інфраструктури.

6. Розробка та впровадження технологічних рішень для виявлення та відсторонення дезінформації. У США діють спеціалізовані технологічні компанії, які використовують штучний інтелект та аналітичні інструменти для виявлення фейків та маніпуляційної інформації. Україна також може інвестувати в розробку сучасних технологій для боротьби з дезінформацією.

7. Регулювання соціальних мереж і платформ, де поширюються дезінформаційні матеріали. Досвід США показує, що співпраця між урядом і технологічними компаніями може призвести до більшої відповідальності та контролю за змістом, який публікується в мережі.

8. Формування законодавства у сфері кібербезпеки. Уряд США активно обговорює можливість прийняття законодавства, яке б регулювало поширення дезінформації та боротьбу з нею. Законодавчі ініціативи можуть включати штрафи для платформ, які не ефективно протидіють дезінформації, або вимоги щодо прозорості у видаленні шкідливого контенту. Нормативно-правова база в Україні, що стосується кібербезпеки потребує значного удосконалення. Досвід США у даному контексті був вельми корисним.

Використання досвіду США в протидії дезінформації може допомогти Україні зміцнити інформаційну безпеку, захистити свою демократію та забезпечити громадянам доступ до об'єктивної та правдивої інформації.

Перспективи подальших досліджень. У боротьбі з дезінформацією США використовують різноманітні стратегії та підходи. Дезінформація є серйозною загрозою для демократії та громадської довіри, тому робота над її протидією важлива і актуальна. Саме тому у контексті перспектив подальших досліджень, на нашу думку, цілком виправданим стала б деталізація змісту і впровадження в сфері боротьби з дезінформацією такого інструменту, як фактчекінг.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] О. Я. Звоздецька, «Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи», *Історико-політичні проблеми сучасного світу*, т. 43, с. 30–39, 2021. [Електронний ресурс]. Доступно: https://mhpi.chnu.edu.ua/index.php/issues/article/view/303/236 Дата звернення: Січ. 10, 2024.

[2] Т. А. Павленко, «Дезінформація: поняття, ознаки, перспективи протидії», *Юридичний науковий електронний журнал*, № 7, с. 337–339, 2022. [Електронний ресурс]. Доступно: https://is.gd/kbAbcN Дата звернення: Січ. 10, 2024.

[3] В. І. Маляренко, «Кращі практики зарубіжного досвіду боротьби з фейками та дезінформацією», *Інформація і право*, № 3(38), с. 21–27, 2021. [Електронний ресурс]. Доступно: https://is.gd/LrZdE3 Дата звернення: Січ. 10, 2024.

[4] Б. М. Андрушків, О. І. Гагалюк, Н. Б. Кирич, О. Б. Погайдак, «Культ-освітня компонента у сфері управління як засіб попередження вульгаризму у взаємовідносинах та поширення фейків в ЗМІ або важелі посилення економічної безпеки в державі», *Вісник економічної науки України*, № 2(37), с. 214–222, 2019. [Електронний ресурс]. Доступно: https://is.gd/ARSOq9 Дата звернення: Січ. 10, 2024.

[5] О. В. Євсюкова, «Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи», *Державне управління: удосконалення та розвиток*, № 2, 2021. [Електронний ресурс]. Доступно: https://is.gd/XCMkaL Дата звернення: Січ. 10, 2024.

[6] Л. А. Арсенович, «Формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади в умовах глобалізації», на *Міжнар. студ. наук. конф. Публічне управління в умовах глобалізації*. Київ, 2018.

[7] Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. USA PATRIOT ACT, *Public Law,* 107-56, oct. 26, 2001. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf Application date: January 12, 2024.

[8] S. Rynning, P. S. Hilde, «Operationally Agile but Strategically Lacking: NATO's Bruising Years in Afghanistan», *LSE Public Policy Review*, vol. 2, ss. 3, pp. 1–11. 2022. https://doi.org/10.31389/lseppr.55

[9] U.S. Code § 3369 – Cooperative actions to detect and counter foreign influence operations. Legal Information Institute. Cornell Law School. [Online]. Available: https://is.gd/coP0RY Application date: January 12, 2024.

[10] A Bill, To make certain modifications relating to the Social Media Data and Threat Analysis Center. H.R. 8409. In the House of Representatives. July 18, 2022. [Online]. Available: https://is.gd/FAsfA5 Application date: January 12, 2024.

[11] H. Res.758, Strongly condemning the actions of the Russian Federation, under President vladimir putin, which has carried out a policy of aggression against neighboring countries aimed at political and economic domination. [Online]. Available: https://is.gd/WzigE1 Application date: January 12, 2024.

[12] Testimony on Ukraine before the House Foreign Affairs Committee. [Online]. Available: https://is.gd/n0KcGo Application date: January 12, 2024.

[13] Countering Information Warfare Act of 2016. [Online]. Available: https://is.gd/iA2pDI; https://is.gd/qe7yxx Application date: January 12, 2024.

[14] *Світова гібридна війна: український фронт*; В. П. Горбуліна, Ред. Харків, Україна : Фоліо, 2017. [Електронний ресурс]. Доступно: http://www.niss.gov.ua/articles/2431/ Дата звернення: Січ. 10, 2024.

[15] Countering Foreign Propaganda and Disinformation Act. [Online]. Available: https://is.gd/i60WYs Application date: January 12, 2024.

[16] National Defense Authorization Act for Fiscal Year 2017. [Online]. Available: https://is.gd/ssQPC2 Application date: January 12, 2024.

[17] Global Engagement Center. [Online]. Available: https://www.state.gov/r/gec/ Application date: January 12, 2024.

[18] Countering America's Adversaries Through Sanctions Act. [Online]. Available: https://is.gd/XiftzX Application date: January 12, 2024.

[19] Rubio, Van Hollen Introduce Legislation to Deter Foreign Interference in American Elections. [Online]. Available: http://bit.ly/2DD4VCX Application date: January 12, 2024.
[20] США направили десятки мільйонів доларів проти пропаганди РФ. [Електронний ресурс]. Доступно: https://is.gd/TZCK1s Дата звернення: Січ. 10, 2024.
[21] INB Newsroom. [Online]. Available: https://is.gd/Sq1OPb Application date: January 12, 2024.
[22] Global Investigative Journalism Network. [Online]. Available: https://gijn.org/ua/resurs-ua/kiberzlochinnist/ Application date: January 12, 2024.

EXPERIENCE OF THE UNITED STATES OF AMERICA CONCERNING COUNTING MISINFORMATION AND POSSIBILITY ITS USE IN UKRAINE

Kuzmenkova Katerina,
Chief consultant of the security department activities
of Commission members Secretariat of the Central Election Commission, Kyiv;
Postgraduate student of the Department of public administration and
Project Management Educational and Scientific Institute
of Management and Psychology
SIHE «University of Educational Management».
Kyiv, Ukraine.
https://orcid.org/0009-0004-7107-8793
20000lpv@gmail.com

Abstract. The article analyzes the experience USA of combating disinformation based on the functioning of the main actors of the US cyberspace. The positive features of the USA related to countering disinformation are identified, namely: conscious and clearly formed understanding of the scope of the disinformation problem; cooperation between different sectors in countering disinformation; effective digital education of citizens, fact-checking and disinformation monitoring; the availability of effective tools and technologies that contribute to the strengthening of cyber protection. An analysis of the activities of government institutions USA and agencies in the field of cyber security was carried out. It is indicated that one of the key aspects of the American experience in countering disinformation is the active role of the government in identifying, analyzing and dispelling disinformation. It is emphasized that the USA has enormous financial, technological, scientific, technical and military potential, and also pays considerable attention to

strengthening national security, protection of citizens' rights and commercial interests in the information sphere. It is noted that the general public task for the USA, which requires joint efforts, is the aggressive policy of Russia and the strengthening of Russian disinformation and propaganda. The possibilities of using the mentioned experience of the American state in Ukraine in such areas as: ensuring transparency in media activities, strengthening international cooperation in the field of cyber security, strengthening critical thinking among citizens and forming media resilience especially in the conditions of Russian intervention, creating and ensuring effective functioning of the Agency have been identified (Center) for countering disinformation, adopting technological solutions for the purpose of identifying and removing disinformation influences, regulating social networks and platforms that spread fakes, rumors and disinformation, establishing and developing the domestic legislation system related to combating disinformation, etc. It has been proven that the fight against disinformation should contribute to the strengthening of democracy, freedom of speech and information security, and the experience of the USA in the field of information management and technologies to fight against disinformation is relevant in today's conditions for Ukraine.

Keywords: misinformation; foreign experience in countering disinformation; fake information warfare; cyber security; cyberspace.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] O. Ya. Zvozdetska, «Dezinformatsiia yak zahroza natsionalnii bezpetsi Yevropeiskoho Soiuzu: problemy ta pidkhody», Istoryko-politychni problemy suchasnoho svitu, t. 43, s. 30–39, 2021. [Elektronnyi resurs]. Dostupno: https://mhpi.chnu.edu.ua/index.php/issues/article/view/303/236 Data zvernennia: Sich. 10, 2024. (in Ukraine)

[2] T. A. Pavlenko, «Dezinformatsiia: poniattia, oznaky, perspektyvy protydii», Yurydychnyi naukovyi elektronnyi zhurnal, № 7, s. 337–339, 2022. [Elektronnyi resurs]. Dostupno: https://is.gd/kbAbcN Data zvernennia: Sich. 10, 2024. (in Ukraine)

[3] V. I. Maliarenko, «Krashchi praktyky zarubizhnoho dosvidu borotby z feikamy ta dezinformatsiieiu», Informatsiia i pravo, № 3(38), s. 21–27, 2021. [Elektronnyi resurs]. Dostupno: https://is.gd/LrZdE3 Data zvernennia: Sich. 10, 2024. (in Ukraine)

[4] B. M. Andrushkiv, O. I. Hahaliuk, N. B. Kyrych, O. B. Pohaidak, «Kult-osvitnia komponenta u sferi upravlinnia yak zasib poperedzhennia

vulharyzmu u vzaiemovidnosynakh ta poshyrennia feikiv v ZMI abo vazheli posylennia ekonomichnoi bezpeky v derzhavi», Visnyk ekonomichnoi nauky Ukrainy, № 2(37), s. 214–222, 2019. [Elektronnyi resurs]. Dostupno: https://is.gd/ARSOq9 Data zvernennia: Sich. 10, 2024. (in Ukraine)

[5] O. V. Yevsiukova, «Osoblyvosti pidhotovky fakhivtsiv u sferi kiberbezpeky: suchasni vyklyky ta perspektyvy», Derzhavne upravlinnia: udoskonalennia ta rozvytok, № 2, 2021. [Elektronnyi resurs]. Dostupno: https://is.gd/XCMkaL Data zvernennia: Sich. 10, 2024. (in Ukraine)

[6] L. A. Arsenovych, «Formuvannia systemy pidhotovky fakhivtsiv u sferi kiberbezpeky orhaniv publichnoi vlady v umovakh hlobalizatsii», na Mizhnar. stud. nauk. konf. Publichne upravlinnia v umovakh hlobalizatsii. Kyiv, 2018. (in Ukraine)

[7] Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. USA PATRIOT ACT, *Public Law,* 107-56, oct. 26, 2001. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf Application date: January 12, 2024. (in English)

[8] S. Rynning, P. S. Hilde, «Operationally Agile but Strategically Lacking: NATO's Bruising Years in Afghanistan», LSE Public Policy Review, vol. 2, ss. 3, pp. 1–11. 2022. https://doi.org/10.31389/lseppr.55 (in English)

[9] U.S. Code § 3369 – Cooperative actions to detect and counter foreign influence operations. Legal Information Institute. Cornell Law School. [Online]. Available: https://is.gd/coP0RY Application date: January 12, 2024. (in English)

[10] A Bill, To make certain modifications relating to the Social Media Data and Threat Analysis Center. H.R. 8409. In the House of Representatives. July 18, 2022. [Online]. Available: https://is.gd/FAsfA5 Application date: January 12, 2024. (in English)

[11] H. Res.758, Strongly condemning the actions of the Russian Federation, under President vladimir putin, which has carried out a policy of aggression against neighboring countries aimed at political and economic domination. [Online]. Available: https://is.gd/WzigE1 Application date: January 12, 2024. (in English)

[12] Testimony on Ukraine before the House Foreign Affairs Committee. [Online]. Available: https://is.gd/n0KcGo Application date: January 12, 2024. (in English)

[13] Countering Information Warfare Act of 2016. [Online]. Available: https://is.gd/iA2pDI; https://is.gd/qe7yxx Application date: January 12, 2024. (in English)
[14] Svitova hibrydna viina: ukrainskyi front; V. P. Horbulina, Red. Kharkiv, Ukraina : Folio, 2017. [Elektronnyi resurs]. Dostupno: http://www.niss.gov.ua/articles/2431/ Data zvernennia: Sich. 10, 2024. (in Ukraine)
[15] Countering Foreign Propaganda and Disinformation Act. [Online]. Available: https://is.gd/i60WYs Application date: January 12, 2024. (in English)
[16] National Defense Authorization Act for Fiscal Year 2017. [Online]. Available: https://is.gd/ssQPC2 Application date: January 12, 2024. (in English)
[17] Global Engagement Center. [Online]. Available: https://www.state.gov/r/gec/ Application date: January 12, 2024. (in English)
[18] Countering America's Adversaries Through Sanctions Act. [Online]. Available: https://is.gd/XiftzX Application date: January 12, 2024. (in English)
[19] Rubio, Van Hollen Introduce Legislation to Deter Foreign Interference in American Elections. [Online]. Available: http://bit.ly/2DD4VCX Application date: January 12, 2024. (in English)
[20] SShA napravyly desiatky milioniv dolariv proty propahandy RF. [Elektronnyi resurs]. Dostupno: https://is.gd/TZCK1s Data zvernennia: Sich. 10, 2024. (in Ukraine)
[21] INB Newsroom. [Online]. Available: https://is.gd/Sq1OPb Application date: January 12, 2024. (in English)
[22] Global Investigative Journalism Network. [Online]. Available: https://gijn.org/ua/resurs-ua/kiberzlochinnist/ Application date: January 12, 2024. (in English)

Стаття надійшла до редакції
10 січня 2024 року