УДК 004.77:323.266
DOI: 10.31673/2409-7292.2024.020010

**Наконечний В. С., Хлевна Ю. Л.,
Половінкін І. М., Кузьменко М. Д.**

МЕТОД ОЦІНКИ РОЗПОВСЮДЖЕННЯ НЕПРАВДИВОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СПЕЦІАЛЬНИХ ПРОГРАМ ТА ТЕХНОЛОГІЙ НА БАЗІ СЕРЕДОВИЩА ІНТЕРНЕТ

Інформаційне протиборство складова частина відносин і форма боротьби сторін, кожна з яких прагне завдати противнику поразку (збитки) у вигляді інформаційних впливів в його інформаційну сферу. Об’єктом інформаційного протиборства може стати будь-який компонент чи сегмент інформаційно-психологічного простору, у тому числі такі види: масова та індивідуальна свідомість громадян; соціально-політичні системи та процеси; інформаційна інфраструктура; інформаційні та психологічні ресурси. Головним методом інформаційного протиборства є розповсюдження неправдивої інформації. Слід звернути увагу, що самі по собі технології не можуть виграти інформаційну війну. Поле бою виходить за межі алгоритмів і коду, сягаючи самої тканини наших суспільств. Аналіз існуючих методів надійного захисту процесу формування громадської думки в мережі Інтернет, показав, що на сьогоднішній день таких методів та технологій немає і бути не може. У статті розглядається актуальне питання розповсюдження неправдивої інформації. Запропоновано метод оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища інтернет. Наведені вирази: для оцінки ефективності застосованої дезінформації та для оцінки відкритості системи управління неправдивої інформації. Це дозволяє зробити кількісну оцінку впливу неправдивої інформації на населення держави та на формування громадської думки взагалі.

Ключові слова: неправдива інформація, метод**,** дезінформація, розповсюдження, фейк, астротерфінг.

Вступ

Поява технологій у масовій комунікації створює нові виклики для України та світу в цілому. Найскладніша і незбагненна річ сучасності – це дезінформація. В Україні немає законодавчого визначення дезінформації. Незважаючи на те, що Закон України «Про інформацію» визначає достовірність і цілісність інформації як один із принципів інформаційних відносин, про цей обов’язок також йдеться в Законах України «Про друковані засоби масової інформації (пресу)» та «Про телебачення і радіомовлення». Але рішенням Ради національної безпеки і оборони України, яке набуло чинності Указом Президента України, у 2021 р. був створений Центр з протидії дезінформації (GPA) в якості робочого органу РНБО. Основна увага Центру зосереджена на протидії поширенню неправдивої інформації та боротьбі з інформаційним тероризмом.

У 2023 році найпопулярнішим джерелом інформації в Україні є Інтернет. Згідно з опитуванням, 62% учасників отримують інформацію з соціальних мереж і 48% з новинних сайтів. Дезінформація може легко поширюватися в соціальних мережах через відсутність редакційного контролю, свободу публікацій для будь-якого користувача та можливість швидко створювати та поширювати інформацію безкоштовно. Користувачі Інтернету можуть легко поширювати вірусний вміст, що призводить до широкого поширення на багатьох сайтах. Отже, сьогодні соціальні мережі набрали величезної популярності, адже там кожен може створювати контент. Дезінформація в Інтернеті цілком свідома. Вона полягає у наданні неправдивої або маніпульованої інформації, що вводить одержувача в оману. Дезінформація створює картину світу, яка не відповідає дійсності. Це призводить до неправильних рішень та дій, а також створює хибне уявлення про конкретну інформацію.

Дезінформація в Інтернеті має на меті надати неправдиву або маніпульовану інформацію, яка повинна мати певний вплив на одержувача. Об'єктом атак можуть стати політичні, соціальні та економічні виміри. Тема дезінформації набирає обертів за умов конфлікту між російською федерацією та Україною. Російська дезінформація зараз є найбільшою загрозою, але не єдиною, з якою ми зіткнемося багато років. Фальсифікація інформації та маніпулювання фактами – це звичайна практика, яку не важко зустріти в Інтернеті. Тому розробка та удосконалення методик та методів оцінки розповсюдження

неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища інтернет є актуальним науковим завданням.

Постановка проблеми

Закономірним наслідком розвитку сучасних технологій та соціальних мереж стало неконтрольоване поширення контенту та підвищення ризиків дезінформації серед суспільства. Загострюється проблема фейкових новин в Інтернеті, робляться спроби припинення розповсюдження неправдивої інформації. Зважаючи на те, що не існує універсального методу виявлення неправдивої інформації, стає важливим вирішення наукового завдання з розробки та удосконалення методів оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища Інтернет. Вирішенню цього завдання присвячено дану роботу.

Аналіз останніх досліджень і публікацій

Поява технологій та соціальних мереж зробила революцію у міжособистісному спілкуванні. Протягом кількох секунд повідомлення або публікація можуть розійтися по всьому світу і можуть бути переглянуті тисячами користувачів. Соціальні мережі набирають популярності, адже там кожен може створювати контент. Зараз 67% американців отримують новини з Facebook.

Вирішенню проблем виявлення та припинення розповсюдження неправдивої інформації присвячено багато публікацій. Так у роботі [1] наведено, що у разі цифровізації визначення меж реалізації права і свободи у кіберпросторі має найважливіше значення. Однак при встановленні таких меж важливо дотримуватися балансу між правом на свободу слова, створенням сприятливого середовища для розвитку нових технологій, необхідністю збереження у кожного користувача доступу до правдивої інформації.

В публікаціях [2–5] розглядається проблема неправдивої інформації у соціальних мережах. Незважаючи на те, що соціальні мережі можуть принести користь, вони мають і зворотний бік. Сьогодні вони перенасичені фейковою інформацією, яку непросто виявити. Згідно з дослідженнями, вона негативно впливає на суспільство. Понад 80% громадян ЄС кажуть, що вони вважають фейкові новини проблемою як для своєї країни, так і для демократії загалом. Але рішення проблеми у цих роботах не наведено.

У роботах [6, 7] розкрита проблема оплачених новин, а саме наведено, що з кожним роком обізнаність аудиторії щодо існування оплачуваних публіцистичних матеріалів зростає: у 2021 році про це знали 83% аудиторії. Більшість вважає, що вони здатні відрізнити одне одного. Так само 83% респондентів знають, що в ЗМІ іноді з'являються фейкові новини та дезінформація. На жаль методам виявлення неправдивої інформації не приділено уваги.

У статтях [8–10] приведені статистичні дані. Опитування, проведене Internews і USAID, показало, що хоча українці кажуть, що вони мало довіряють російським ЗМІ – одному з основних джерел дезінформації, – їх здатність виявляти фейкові новини залишається низькою. Згідно з дослідженням, 65% українців заявили, що можуть відрізнити фейкові новини від справжніх. Однак при тестуванні на трьох реальних прикладах лише 11% цих людей точно ідентифікували всі фейкові новини. Наведена статистика свідчить о необхідності створення методик по виявленню неправдивої інформації у Інтернеті.

Суттєвим аспектом проблеми є нездатність пошукової технології виявити, з інформаційного простору, сумнівний зміст і визначити правдивість інформації. Існуючи методи не повною мірою враховують темпи розвитку інформаційних технологій та, відповідно, рівень інформаційного впливу на суспільство тому актуальним є наукове завдання по розробки та удосконалення методів оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища інтернет.

Виклад основного матеріалу

Будь-яка інформаційна операція, операція по дезінформації завжди спрямована зміну картини світу противника, на досягнення очікуємого результату. Зміна картини світу, своєю

чергою, передбачає коригування знання противника. Коригувати знання, яке втілюється у структурі системи та функціональних можливостях елементів цієї структури, означає коригувати саму структуру, тобто:

включати до неї нові елементи;

виключати елементи;

модифікувати зв'язки між елементами.

Неправдива інформація, завжди спрямована перепрограмування противника. Для боротьби проти неправдивої інформації не існує типової стратегії. Кожен противник заслуговує на індивідуальний підхід, що максимально враховує його особливості щодо сприйняття інформації [11]. Для соціальних систем потрібне знання історії народів, культури, звичаїв, але в насамперед − принципів і найдокладніших нюансів щодо функціонування та формування системи управління. Для технічних систем − способи інформаційного впливу, мова, особливості архітектури, «люки» в системі захисту та, звичайно, алгоритми роботи системи управління.

Неправдива інформація це інформаційна зброя, яка являє собою технічні засоби і технології, виробництво яких поставлено на промислову основу, що застосовуються для активізації, знищення, блокування або створення в інформаційній системі процесів, в яких зацікавлений суб'єкт, що застосовує зброю.

Основою принципу функціонування інформаційної зброї є запуск або генерація програми самообмеження, властивої будь-якій складній інформаційній системі, здатної до навчання. Завдання розповсюдження неправдивої інформації полягає лише в тому, щоб, маніпулюючи вхідними даними, активізувати в системі-жертві необхідні програми або процеси, що призводять до генерації таких програм. Отже, йдеться про створення заданих алгоритмів шляхом маніпулювання вхідними даними, тобто шляхом коригування описів об'єктів.

При чому, особливістю є те, що дані алгоритми функціонують у потенційному середовищі жертви за рахунок її коштів, чи то технічна сфера, чи гуманітарна.

Кінцева мета застосування неправдивої інформації та дезінформації – сфера управління.

Для оцінки ефективності застосованої дезінформації можливо використовувати наступний вираз:

$$f = n\, s / t\, (d+v), \qquad (1)$$

де:

n – кількість людей або технічних засобів, яких ця дезінформація здатна перепрограмувати;

s – площина або ареал, на якій перепрограмування стає можливим;

t – інтервал часу, протягом якого люди або технічні засоби можуть бути перепрограмовані;

d – вартість виготовлення одиниці дезінформації;

v – накладні витрати (оплата роботи тих, хто застосовує зброю).

Інформаційна зброя за своїм впливом охоплює більшість населення планети. При цьому потенційні жертви самі оплачують виробництво та доставку до себе додому коштів для власного перепрограмування на чуже замовлення. Накладні витрати на цей вид озброєння мінімальні. Сплатити потрібно лише кілька десятків телевізійних каналів, які охоплюють своєю дією весь світ, інше сплатять самі жертви. Час створення та трансляції замовленої передачі вимірюється навіть не годинами, а часом хвилинами. І на відміну від ядерного, дія інформаційного може бути цілеспрямованою. Отже, ідеалу досягнуто. Залишилося вдосконалювати прийоми та визначатися з цілями. Єдине, що тут ще потрібно, це захопити

© Наконечний, В. С., Хлевна, Ю. Л., Половінкін, І. М., & Кузьменко, М. Д. (2024). Метод оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища Інтернет. Сучасний захист інформації, 2(58), 84–90. https://doi.org/10.31673/2409-7292.2024.020010.

монополію на виробництво базового програмного забезпечення, призначеного для розумних систем.

Астротерфінг як загроза інформаційній безпеці

Астротерфінг – створення штучної громадської думки за допомогою спеціальних програм та технологій на базі середовища Інтернет. Інтернет – це не тільки засоби масової інформації, які складаються з взаємодіючих технічних систем, це середовище у якому одночасно мешкають як люди, так і програмні модулі, які мало чим відрізняються від людей.

Класичним прикладом інформаційної зброї у технічній сфері є бот мережі (ботнети). Ботнет (англ. botnet, походить від слів robot і network) - це комп'ютерна мережа, що складається з хостів та комп'ютерів користувачів із встановленим на ній спеціальним програмним забезпеченням (бот), управління яким здійснюється з хостів. У мережи Інтернет, наводиться приклад коли Нідерландська поліція захопила 30-мільйонний ботнет. Тільки за один місяць прихованого спостереження за його активністю мережа поповнилася трьома мільйонами заражених машин. Ботнет був частиною мережі Bredolab. Bredolab - це велика родина троянських програм, що проникають на комп'ютери користувачів через шкідливі програми до поштових повідомлень або заражені сайти. Отримавши контроль над комп'ютером, Bredolab завантажує інші шкідливі програми. Добре відомо про зв'язок Bredolab зі спамерськими розсилками та лже-антивірусами. У ході розслідування було виявлено 143 контролюючі сервери. У ході знищення ботнета контролюючі сервери було відключено від Мережі.

Бот мережа включає центр управління, з якого надходять команди, та безліч заражених комп'ютерів. Зрозуміло, що якщо центр виявлено, то мережа ставиться під контроль або знищується.

Боти (заражені комп'ютери) отримують із центру команди для виконання. Команда складається з переліку дій та часу виконання, типу:

зайти на сайт Z (час: від T_1 до T_2);

надіслати листа за адресою X (час: від T_1 до T_2);

знімати інформацію з папки P, клавіатури, тощо і переміщати у сховище M (час: від T_1 до T_2);

надіслати зібрані дані до сховища M за адресою X (час: від T_1 до T_2);

впровадити заражений код Dk за заданими адресами $\{X_i\}$ (час: від T_1 до T_2);

отримати дані D (наприклад, Dk) за адресою X та зберігати в місці M (час: від T_1 до T_2);

змінити адреси центру керування $\{X_i\}$ на адреси $\{Y_i\}$ (час: від T_1 до T_2);

змінити ключ шифрування (час: від T_1 до T_2);

доповісти про виконання команди (час від T_1 до T_2);

«заснути» (тимчасово: від T_1 до T_2);

самознищення (час: від T_1 до T_2) і т.д.

Команди під час передачі ботам шифруються криптографічним алгоритм з відкритим ключем RSA. Відкритий ключ є у кожного бота закритий тільки в центрі управління. Таким чином здійснюється захист ботів від захоплення потенційними противниками. Існують ботнети з фіксованим центром управління та з центром, що динамічно змінюється. Динамічно змінюється центр управління створюється самими ботами, які шляхом генерації випадкової послідовності, наприклад, застосовуючи американський DES до деякого тексту, випрацюють послідовність адрес $\{X_i\}$, на яких намагаються розмістити центр управління у вигляді команд D. У разі вдалого зараження комп'ютера боти надалі використовують його зв'язок з власником мережі. Власник ботнета, знаючи правила генерації випадкової послідовності, завжди може зв'язуватися з ботами через будь-який з комп'ютерів центру управління, які постійно змінюються. У яких випадках це необхідно. Це необхідно у випадках:

виявлення зараженого комп'ютера антивірусом;

виявлення зараженого комп'ютера через попадання в руки потенційного супротивника бота з адресами;

зараження нових комп'ютерів.

Ступінь можливого ураження системи управління безпосередньо пов'язані з відкритістю системи, тому наступний етап дослідження — кількісна оцінка відкритості системи управління супротивника, що є найважливішою характеристикою ступеня розповсюдження неправдивої інформації, дезінформації та загалом інформаційного впливу.

Спробуємо розробити кількісну оцінку інформаційного впливу.

Зробимо припущення, нехай: $X = \{x_1, x_2, \ldots x_n\}$ – суб'єкти, що належать системі управління. Кожен із них може бути охарактеризований близькістю до основного центру ухвалення рішень $\{s_i\}$. Наприклад, $s_i = 5$ – особа, яка приймає рішення, $s_i = 4$ – безпосередній постійний контакт з особою, яка приймає рішення, $s_i = 3$ – безпосередній періодичний контакт, $s_i = 2$ – опосередкований (через одного) постійний контакт, $s_i = 1$ – опосередкований (через одного) періодичний контакт, $s_i = 0$ – відсутність безпосередніх контактів.

Крім того, кожен із названих суб'єктів може бути охарактеризований з позиції близькості його до зарубіжних культур (навчання у відповідних зарубіжних центрах, близькості до життєвих інтересів інших держав (наявність родичів та друзів, які живуть та працюють за кордоном або у фірмах, що мають в основному іноземний капітал)) Зрозуміло, що дана характеристика стосовно конкретного суб'єкта не може говорити про те, що даний суб'єкт є «агентом впливу», але у своїй сукупності (по всій системі управління) цілком може виступати як певна оцінка ступеня її відкритості.

Тоді як що ми позначимо через τ_i – оцінку близькості індивіда до «чужих» життєвих інтересів та культур (у тому числі кримінальних). Далі будемо враховувати, наступне, припущене, а саме:

Нехай:

$\tau_i = 5$ – громадянин іншої країни;

$\tau_i = 4$ – робота за кордоном;

$\tau_i = 3$ – близькі родичі за кордоном;

$\tau_i = 2$ – друзі та постійні знайомі там;

$\tau_i = 1$ – часті поїздки за кордон;

$\tau_i = 0$ – закордонних контактів немає.

Тоді ступінь відкритості окремо взятого суб'єкта буде визначатися виразом :

$$C_i = \tau_i s_i/25, \tag{2}$$

а всієї системи управління:

$$B = \Sigma \tau_i s_i/25. \tag{3}$$

Таким чином вираз (3) дає можливість оцінити у числовому значені відкритість системи управління. Зробимо графічне представлення отриманих результатів. Графічне представлення результатів наведено на рис. 1.

Як бачимо з результатів математичного моделювання оцінити у вигляді графічного представлення відкритості системи управління, зі зростанням близькості до центру ухвалення рішень та зростанням наближення індивідів до правдивої інформації. Відкритість системи управління потоками інформації зростає, що цілком підтверджує результати теоретичних розрахунків та адекватність запропонованого методу оцінки розповсюдження неправдивої інформації.

Відкритість системи управління показує можливий кількісний вплив неправдивої інформації або дезінформації на інформаційну безпеку держави. У літературі є приклад того

що при наявності 100 тис. роботів, можливо ініціювати будь-яку законодавчу ініціативу, створити громадську думку або змінити її. Таким чином, найважливішим завданням забезпечення інформаційної безпеки держави є пояснення користувачам Інтернету того факту, що настав час, коли до всього, що відбувається в Інтернеті, щодо формування громадської думки, треба ставитися з певною часткою недовіри.

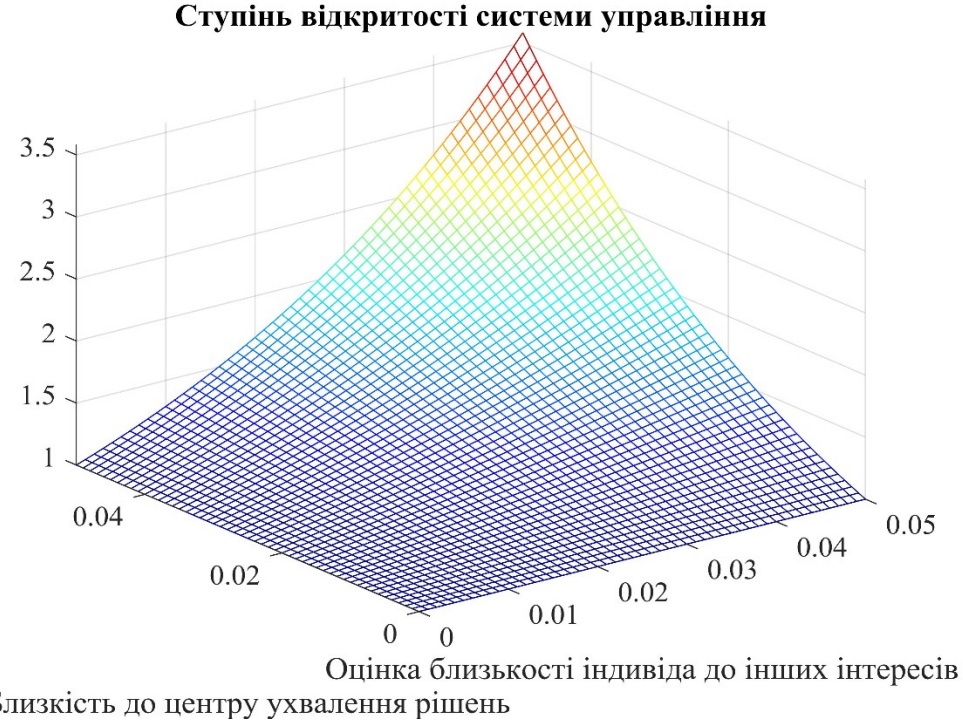

Рис.1. Графік відкритості системи управління

Вплив на громадську думку, як і захист її, – це одне з найактуальніших сучасних завдань, які стосуються забезпечення інформаційної безпеки держави.

Висновок:

Проведене дослідження довело, що громадська думка на базі ресурсів Інтернет є сукупністю взаємопов'язаних індивідуальних думок з конкретного питання, що стосується групи людей. Ці думки зафіксовані на ресурсах мережі Інтернет. Новина є тим вузлом, який збирає ці думки навколо себе. Через систему управління можливо впливати на соціум держави. Саме через відкритість системи управління ресурсами дозволяє розрахувати вплив на соціум. Аналіз існуючих методів надійного захисту процесу формування громадської думки в мережі Інтернет, показав, що на сьогоднішній день таких методів та технологій немає і бути не може. Наведені вирази: для оцінки ефективності застосованої дезінформації та для оцінки відкритості системи управління неправдивої інформації. Це дозволяє зробити кількісну оцінку впливу неправдивої інформації на населення держави та на формування громадської думки взагалі.

Метод оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища Інтернет суттєво допоможе у виявлення та блокування неправдивої інформації, що є головним завданням забезпечення інформаційної безпеки держави.

© Наконечний, В. С., Хлевна, Ю. Л., Половінкін, І. М., & Кузьменко, М. Д. (2024). Метод оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища Інтернет. Сучасний захист інформації, 2(58), 84–90. https://doi.org/10.31673/2409-7292.2024.020010.

Перелік посилань

1. Savchenko, V., Ilin, O., Hnidenko, N., Tkachenko, O., Laptiev, O., Lehominova, S. Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025.
2. Гнатієнко, Г. М., Снитюк, В. Є. Експертні технології прийняття рішень. − К.: McLaut, 2008. − 444 с.
3. Schefer-Wenzl, S., Strembeck, M. Modeling support for role-based delegation in process-aware information systems. Business and Information Systems Engineering. 6 (4). 2014. pp. 215-237. DOI: 10.1007/s12599-014-0343-3
4. Лаптєва, Т. Алгоритм визначення міри існування недостовірної інформації в умовах інформаційного протиборства. Кібербезпека: освіта, наука, техніка. No 2 (14), 2021, с. 15-25. DOI 10.28925/2663-4023.2021.14.1525, ISSN 2663-4023.
5. Лукова-Чуйко, Н., Лаптєва, Т. Виділення та відбір ознак для визначення неправдивої інформації. V Міжнародна науково-практична конференція. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)"27-28 жовтня 2022 р. Київ, Україна. Збірник матеріалів доповідей та тез. С 13-15.
6. Лаптєв, О. А., Бабенко, Р. В., Правдивий, А. М., Зозуля, С. А., Стефурак, О. Р. Удосконалена методика вибору послідовності пріоритетів обслуговання потоків інформації. Науково-практичний журнал «Зв'язок». К.: ДУТ, 2020. №4 (146), С.27 – 31.
7. Наконечний, В., Лаптєв, О., Погасій, С., Лазаренко, С., Мартинюк, Г. Відбір джерел з неправдивою інформацію методом бджолиної колонії. Наукоємні технології. Інформаційні технології, кібербезпека. Том 52 № 4 (2021) С.330-337. DOI: https://doi.org/10.18372/2310-5461.52.16379
8. Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S., Laptieva, T. Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Кібербезпека: освіта, наука, техніка. Том 4 № 12 (2021): pp.19-28.
9. Citron, D. K. Cyber mobs, disinformation, and death videos: the Internet as it is (and as it should be) Michigan Law Review. – Ann Arbor, 2020. – Vol. 118, N 6. pp. 1073–1094.
10. Лаптєва, Т. О. Методика виявлення неправдивої інформації для безпеки Держави. Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень» 23-24 листопада 2023 р. Київ. Україна. С.131–132.
11. Pesetski, A. Deepfakes: a new content category for a digital age. William & Mary bill of rights journal. – Lexington, 2020. – Vol. 29, N 2. pp. 503–532.

Надійшла 11.05.2024