

Visn. Lviv. Univ., Ser. Zhurn. 2025: 56; 194–207 • DOI: <http://dx.doi.org/10.30970/vjo.2025.56.13273>

УДК 070.4[316.774:004]+ [007 : 304 : 659.3](477)

ДЕЗІНФОРМАЦІЙНІ ТЕХНІКИ ШАХРАЙСТВ НА ТЕМІ ВОЛОНТЕРСТВА В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Романюк Альона

*Навчально-науковий інститут журналістики
Київського національного університету імені Тараса Шевченка
вул. Володимирська, 64/13, 01601, Київ, Україна
e-mail: aliona.romaniuk@knu.ua
<https://orcid.org/0009-0008-8127-8675>*

Шевченко Вікторія

*Навчально-науковий інститут журналістики
Київського національного університету імені Тараса Шевченка
вул. Володимирська, 64/13, 01601, Київ, Україна
e-mail: victoryshe@knu.ua
<https://orcid.org/0000-0003-1642-1283>*

У статті розглянуто дезінформаційні техніки, на яких будуються шахрайські схеми, пов'язані із волонтерством під час російсько-української війни. Автори дослідили опубліковані в медіа матеріали щодо збору коштів волонтерськими організаціями чи персоналіями в умовах російського вторгнення в Україну і розробили класифікацію шахрайських схем. У статті наводяться приклади шахрайських схем та дезінформаційних технік, які лежать в їхній основі, а також запропоновано рекомендації щодо перевірки волонтерських проєктів на наявність дезінформації.

Ключові слова: дезінформація, шахрайство, медіа, соціальні мережі, волонтерство, російсько-українська війна, інформаційні кампанії, маніпуляція.

1. Постановка проблеми.

Актуальність теми. В умовах російсько-української війни волонтерство стало справжнім феноменом українського суспільства та підтримки Збройних Сил України, об'єднання громадян навколо спільних цілей та ідеї перемоги. Більшість волонтерських зборів відбувається у форматі онлайн з використанням соціальних мереж, месенджерів, онлайн-банкінгу, персонального бренду та месенджерів. У таких реаліях волонтерство не тільки об'єднує спільноту, його також широко використовують шахраї для особистого збагачення. Саме шахрайські схеми складають основу дискредитаційних кампаній, які вводять людей, різні суспільні групи, в оману, підбивають не тільки волонтерські збори, але й дестабілізують українське суспільство.

Тему шахрайства та спекулювання на темі волонтерства широко висвітлюють правоохоронні органи, журналісти, фактчекери, блогери та громадські організації, проте це не зменшує рівень шахрайства, що своєю чергою породжує недовіру до волонтерства загалом. Враховуючи масштаби волонтерського руху в Україні, швидкість поширення дезінформації в медіа, лояльний підхід до регулювання волонтерства на законодавчому рівні, шахрайські схеми, використовуючи техніки дезінформації, впливають на інформаційну безпеку України. Попри великий обсяг досліджень, присвячених, зокрема, феноменам дезінформації і шахрайства, взаємозв'язок між цими явищами у контексті волонтерської діяльності в умовах війни залишається маловивченим.

Мета статті полягає у класифікації шахрайських схем з дезінформацією на тему волонтерства та напрацювання рекомендацій щодо визначення ознак дезінформації у псевдоволонтерських зборах. Для досягнення мети статті було окреслено такі завдання:

1. Окреслити поняття шахрайства, визначити основні дезінформаційні техніки шахрайських схем під час повномасштабного вторгнення РФ в Україну.
2. Проаналізувати згадки у медіа про шахрайства на темі волонтерства за 2022-2024 рр.
3. Класифікувати шахрайські схеми відповідно до рівнів дезінформаційних технік.
4. Окреслити рекомендації щодо підвищення стійкості суспільства та індивідумів до шахрайських впливів на темі волонтерства.

2. Аналіз останніх досліджень.

Шахрайство в Україні здебільшого розглядають у юридичному та економічному аспектах. Наприклад, корпоративне та фінансове шахрайство досліджують Г. Чернишов, Т. Климко, Л. Маршук, Т. Кізима, О. Стецюк, М. Шаповалов, С. Заболотна та інші. Відповідальність за шахрайські дії вивчають О. Гумін, А. Бабенко, М. Палій, В. Тихий, О. Кушнарєва. Проблема шахрайства під час війни пов'язана також із тим, що знайти шахраїв і притягнути їх до відповідальності складно, адже інтернет-мережа здатна анонімізувати процес шахрайства й тих, хто створює і поширює шахрайські схеми.

Серед наявних розвідок на увагу заслуговує праця І. Чекмарьової, яка досліджує шахрайство в інтернеті як один із видів шахрайства. З-поміж іншого вона пише також про види шахрайств через інтернет, які відбуваються в умовах війни, і наводить такі приклади, як збір коштів для військових, шахрайства, пов'язані з оголошеннями про зникнення рідних або їхнє потрапляння в полон, а також обманні схеми, які використовують фейкові повідомлення про евакуацію за умови передплати або про фінансову допомогу¹. О. Брисковська і М. Гемелей звертають увагу на найбільш поширені шахрайські схеми під час війни: шахрайство щодо збору грошей на ЗСУ або на авто для ЗСУ, фейкові збори коштів на лікування дітей, які постраждали від війни, фейкове отримання міжнародної допомоги, фейкове перевезення біженців та допомога з житлом, продаж неіснуючих товарів і послуг у інтернет-крамницях,

¹ Чекмарьова, І.М. (2024), «Шахрайство в Інтернеті як один із видів шахрайства». *Аналітично-порівняльне правознавство*, Ужгород, 2, с. 639-643. URL: <http://surl.li/skxqxx> (останній перегляд 09 грудня 2024).

шахрайство тощо². Я. Левківська акцентує на впливі воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні³.

Попри велику кількість досліджень, пов'язаних із шахрайством, у науковій літературі практично немає розвідки щодо аналізу шахрайських схем, поширюваних у медіа і пов'язаних саме із волонтерством як унікальним феноменом під час російсько-української війни.

3. Методологічна основа дослідження.

Для досягнення мети і завдань цієї статті застосовано комплекс методів, зокрема бібліографічно-семантичний використано для встановлення термінологічної відповідності у матеріалі та пояснення взаємозв'язку між шахрайськими схемами на волонтерстві та дезінформаційними тактиками як невід'ємною частиною шахрайств, метод аналізу використано для дослідження шахрайських схем, зокрема тих, про які йдеться на офіційних ресурсах Кіберполіції, Національного банку України, Центру протидії дезінформації, фактчекінгових ресурсах, що виявляють шахрайські схеми, як-от «НотаЄнота» та «Без брехні», а також у загадках про шахрайські схеми у медіа.

За допомогою методу інтерв'ю було зібрано інформацію про шахрайські схеми із військовими волонтерками, зокрема Марією Кісіль, а також 20 учасницями літньої школи ВолонтеркиUA, що проходила у с. Татарів у серпні 2024 р. Метод узагальнення та систематизації застосовано для визначення типів шахрайських схем на основі дезінформаційних ознак повідомлень. Важливою частиною дослідження є розробка рекомендацій для громадян щодо виявлення інформаційних загроз і попередження оман, що ґрунтується на темі волонтерства.

4. Виклад основного матеріалу дослідження.

З початком повномасштабного вторгнення в Україні зросла активність шахраїв загалом і шахраїв в онлайн-просторі зокрема. Користуючись ситуацією, ростом руху волонтерства в Україні та складним становищем громадян, злочинці адаптують шахрайські схеми під сьогодення та вводять в оману людей за допомогою певних легенд або історій, вибудованих на дезінформації.

Для досягнення поставленої мети варто виокремити поняття шахрайства, волонтерства та дезінформації, які нерозривно пов'язані в контексті російсько-української війни.

Кримінальний кодекс України визначає шахрайство як «заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою»⁴. Міжнародна організація міграції під поняттям шахрайства розуміє «спотворення або приховування суттєвих фактів з метою обману та отримання несанкціонованої вигоди». Як приклади деяких шахрайських схем, структура наводить навмисні оманливі дії, підробку документів, приховування певної інформації, неправдиве представлення чогось або когось, проте визначальним фактором є намір отримати

² Брисковська, О. М., & Гелемей, М. О. (2023), «Особливості вчинення шахрайства в мережі інтернет в умовах воєнного стану», *Київський часопис права*, 3, с. 174–180.

³ Левківська, Я. В. (2022), «Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні», *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття*, Т. 2, Видавничий дім «Гельветика», Одеса, с. 521–523.

⁴ Кримінальний кодекс України (2024), URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (останній перегляд 09 грудня 2024).

вигоду фінансову, майнову чи у вигляді послуг⁵. Своєю чергою Асоціація сертифікованих фахівців із розслідування шахрайства (ACFE) зазначає, що є три види шахрайських схем відповідно до типізації за жертвами: індивідуальні шахрайства, внутрішнє організаційне шахрайство та зовнішнє організаційне шахрайство⁶.

Щоб коректно виокремити дезінформаційні аспекти шахрайських схем у контексті волонтерства, варто розглянути поняття волонтерства відповідно до українського законодавства. Закон України «Про волонтерську діяльність» визначає волонтерство як форму благодійності, а також як «добровільну, соціально спрямовану, неприбуткову діяльність, що здійснюється волонтерами шляхом надання волонтерської допомоги». Під волонтерською допомогою варто розуміти «певну роботу та послуги, що безоплатно виконуються і надаються волонтерами»⁷. Автори посібника волонтера зазначають, що одним із факторів волонтерської діяльності є те, що вона не примусова, тобто базується виключно на власних переконаннях, прагненнях та особистій мотивації, а вища мета волонтерства – це «створення суспільства, в якому кожен зможе відчути себе в безпеці та під захистом правосуддя»⁸. Саме розуміння цієї мети та прагнення людей бути корисними складають основу шахрайських схем, пов'язаних із волонтерством.

Організація Північноатлантичного договору (НАТО), яка має окремий напрямок протидії дезінформації, терміном «дезінформація» охоплює широкий спектр тактик, методів і процедур і як синонім використовує термін «ворожа інформаційна діяльність». За визначенням НАТО, дезінформація – навмисне створення і поширення неправдивої або маніпульованої інформації з метою обману або введення в оману⁹.

Серед ознак дезінформаційних кампаній дослідниця Т. Павленко визначає імітаційність, тобто подання матеріалу як правдивого, а також «вбудованість» у певні системи поглядів, відповідність певним переконанням. Вона зазначає, що «дезінформація стосується певних переконань, відповідає певній системі поглядів, прив'язана до соціально значущих подій, тобто суспільно важливої інформації, що є чутливою або має символічну цінність»¹⁰.

Таким чином, можемо вказати на зв'язок між дезінформацією та шахрайством, адже в основі шахрайських схем – обов'язкове введення в оману, тобто дезінформаційні аспекти повідомлень, спрямованих на аудиторію та конкретних потенційних жертв.

⁵ Міжнародна організація міграції (2024), «Шахрайство, корупція та неправильне використання ресурсів», URL: <http://surl.li/ywuhq> (останній перегляд 09 грудня 2024).

⁶ ACFE (2024) «Fraud 101: What Is Fraud?». URL: <http://surl.li/gnlas> (останній перегляд 09 грудня 2024).

⁷ Закон України «Про волонтерську діяльність» (2024). URL: <https://zakon.rada.gov.ua/laws/show/3236-17#Text> (останній перегляд 09 грудня 2024).

⁸ Вашкович, В. В., Василенко, О. Ю., Карабін, Т. О., Лазур, Я. В., Манзюк, В. В. та Рошканюк, В. М. (2022), *Посібник волонтера*, Видавничий дім «Гельветика», Одеса, 88 с. URL: <http://surl.li/fwtxgc> (останній перегляд 09 грудня 2024).

⁹ Організації Північноатлантичного договору (2024), «Підхід НАТО у галузі боротьби з дезінформацією». URL: https://www.nato.int/cps/uk/natohq/topics_219728.htm (дата звернення: 9.12.2024).

¹⁰ Павленко, Т. А. (2022), «Дезінформація: поняття, ознаки, перспективи протидії», *Юридичний науковий електронний журнал*, (7), с. 337–339.

За результатами дослідження Національного банку України та Опендатаботу, станом на 9 жовтня 2023 р. 11% українців ставали жертвами шахраїв від початку повномасштабного вторгнення¹¹. Попри таку кількість жертв шахраїв, тільки 18% справ про шахрайство доходять до суду. 2023 рік став рекордним за кількістю випадків шахрайства, які зафіксували правоохоронці. За даними Генпрокуратури, наданими на запит Опендатаботу, було відкрито 82 тисячі проваджень, 18% з яких зрештою дійшли до суду. Порівняно з 2022 р. зловмисники намагалися ошукати українців майже втричі частіше¹².

Проаналізувавши згадки у медіа про шахрайства на темі волонтерства за 2022–2024 рр., дослідивши контент фактчекінгових проєктів «НотаЄнота» щодо шахрайських схем, а також на основі інтерв'ю із військовими волонтерками, учасницями літньої школи ВолонтеркиUA, ми виокремили такі **типи шахрайських схем** відповідно до того, від імені кого вони поширюються:

1. Шахрайство від імені «військових».
2. Шахрайство під гаслом благодійного фонду.
3. Шахрайство від імені конкретного волонтера.
4. Шахрайські схеми від контрагентів, з якими працюють волонтери.
5. Шахрайські схеми від імені донаторів, благодійників та банків.

Шахрайські схеми від імені справжніх чи вигаданих військових можна поділити на два підтипи:

- Шахрайські схеми, в яких беруть участь справжні або колишні військові. До цього підтипу належать випадки, коли, наприклад, військовий – у СЗЧ (самовільному залишенні частини) і збирає гроші на власні потреби.
- Шахрайські схеми, в яких шахраї видають себе за військових. Тобто людина називає себе військовим, але таким не є. Прикладами такого типу шахрайств можна вважати випадки, коли псевдовійськові збирають гроші у людних місцях (так звані «ряжені військові»), коли шахраї в інтернеті видають себе за військових і пишуть повідомлення у месенджерах з проханнями допомогти коштами або роблять окремі збори від чужого або вигаданого імені.

Шахрайські схеми від імені благодійних фондів, значна кількість яких виникла після російського вторгнення в Україну у 2014, а також різко збільшилася у 2022 році. Як вказано у соціологічному дослідженні «Громадянське суспільство в Україні в умовах війни – 2022», громадським і благодійним організаціям вдалося залучити і адмініструвати значні ресурси, що дало змогу посилити українську армію, згуртувати суспільство і дещо пом'якшити ситуацію населення, яке потерпає від війни¹³. Саме тому шахраї використовують прикриття благодійними фондами, щоб отримувати кошти. Такі схеми мають щонайменше три підтипи:

- Шахрайські схеми, пов'язані зі звітністю. Наприклад, це можуть бути справжні благодійні фонди, які справді зареєстровані, збирають кошти, але, наприклад,

¹¹ Opendatabot (2024), «Кожен дев'ятий опитаний українець ставав жертвою шахраїв від початку повномасштабного вторгнення». URL: <https://opendatabot.ua/analytics/stopfraud-nbu> (дата звернення: 9.12.2024).

¹² Там само.

¹³ Громадянське суспільство в Україні в умовах війни (2023). Звіт за результатами дослідження, Київ, 64 с. URL: <http://surl.li/fywzkh> (останній перегляд 09 грудня 2024).

велика кількість коштів йде на операційну діяльність або інші статті витрат. Відповідно до Закону України «Про благодійну діяльність та благодійні організації», «розмір адміністративних витрат благодійної організації не може перевищувати 20% доходу цієї організації у поточному році»¹⁴. За даними Оpendatabot, у 2023 р. 76% (понад 22 тисячі благодійних організацій) не подали звітності до Держстату. Найчастіше не подають звітності ті організації, що надають соціальну допомогу (87%), займаються освітою (6,8%), а також незначний відсоток громадських організацій (4,3%)¹⁵. Інший приклад цього підтипу шахрайства, коли організації подають фотозвіти у соціальних мережах, але не подають звіти про зібрані і витрачені кошти. У таких випадках створюється ілюзія допомоги, але фактична допомога постраждалим від бойових дій відрізняється від суми зібраних коштів.

- Шахрайські схеми, в яких шахраї виступають від імені відомих благодійних фондів. Наприклад, коли створюють фейкові сайти або сторінки у соціальних мережах від імені фонду «Повернись живим», «Фонду Сергія Притули», фонду «Save the children» та інших. У таких випадках шахраї задіюють метод, який часто використовують у дезінформаційних кампаніях, – метод підкріплення авторитетом. Впізнаваність бренду і недостатня уважність людей сприяє ефективності цього типу шахрайських схем.
- Шахрайські схеми, в яких шахраї виступають від імені неіснуючих фондів. Від імені таких неіснуючих фондів шахраї обдзвонюють людей та організації з проханням допомогти. Учасники таких шахрайських схем працюють за певним алгоритмом, маючи заготовлені варіанти відповіді на заперечення та питання потенційних жертв. Зараз такі схеми менш поширені, адже з 2022 р. чимало медіа та офіційних структур поширювали пам'ятки, як зрозуміти, що благодійний фонд несправжній.

Від імені волонтерів відбувається чи не найбільше і справжніх, і шахрайських зборів. З одного боку, чи не кожна сім'я в Україні має рідних та близьких у лавах ЗСУ, а тому і долучається до зборів, і волонтерить. Проте, з іншого боку, саме цю поширеність волонтерського руху і використовують шахраї. Загалом усі схожі шахрайські схеми можна згрупувати у три види:

- Волонтери, які справді збирають кошти, але не звітують або звітують не за усю зібрану суму, не надають чеків, виписок та зведеного бюджету – скільки збрали і скільки витратили. Такі шахрайські схеми підривають довіру до культури волонтерства в Україні загалом.
- Люди, які були волонтерами і припинили волонтерську діяльність, проте користуються своїм іменем і впізнаваністю для збору коштів. Прикладом такого кейсу може слугувати історія, пов'язана із медичним батальйоном України «Госпітальєри», усі працівники якого – волонтери. Колишня співробітниця благодійного фонду Анна Скольбушевська із ніком «адмірал Няв», яка оголошувала збори на допомогу військовим, витрачала донати на азартні ігри та влас-

¹⁴ Закон України «Про благодійну діяльність та благодійні організації» (2024). URL: <https://zakon.rada.gov.ua/laws/show/5073-17#Text> (останній перегляд 09 грудня 2024).

¹⁵ Opendatabot (2024), «76% благодійних організацій не подають фінзвітність». URL: <https://opendatabot.ua/analytics/foundation-go-financial-reports> (дата звернення: 9.12.2024).

ний відпочинок. Дівчина через соцмережу X неодноразово збирала донати не тільки для «Госпітальєрів», але й для інших фондів. Наприкінці червня 2024 р. користувачі X помітили проблеми у звітах Адмірала Няв. Наприклад, зі збору на турнікети без пояснень зняли 3 тисячі гривень, а зі збору на системи для переливання крові – 166 тисяч гривень без звіту. Обіцяний розіграш за донат сертифікату Stop the Bleed не провели, а після закриття банки Анна пообіцяла відвідувати «за кілька годин», але зникла. «Госпітальєри» повідомили, що Скольбушевська не працює в їхньому фонді ще з грудня 2023 р. Важливо зазначити, що дівчина вказувала медичний батальйон в описі своєї сторінки та проводила збори. Щодо ймовірного шахрайства Скольбушевської зареєстрували кримінальне провадження¹⁶.

- Шахраї, які видають себе за волонтерів, а також за рідних або близьких військових. Прикладом цього типу шахрайств є фейкові сторінки у соціальних мережах, які збирають кошти на ЗСУ, на автівки для конкретних підрозділів, для порятунку дітей, собак або конкретні потреби постраждалих внаслідок російських атак на українські населені пункти. Найпоширеніші випадки таких шахрайських схем відбуваються після обміну військовополоненими, після повернення українських військових з російського полону. Шахраї використовують справжні фото та історії, а також імена рідних, від чийого імені збирають кошти на картки. Приклади таких шахрайських схем і фейкових зборів фіксують активісти з фейсбук-групи «Стоп шахрайство».

Шахрайські схеми від контрагентів, із якими працюють волонтери, також доволі поширені. Волонтери отримують прохання від військових щодо потреби на фронті. Після цього шукають, де можна придбати і скільки це коштує. Відповідно, після дослідження ринку і отримання попередніх домовленостей щодо закупівлі, волонтери відкривають збір коштів. Волонтери – це одна з цільових аудиторій шахраїв, зокрема тих, хто імітує продаж товару (часто такий товар закуповують за кордоном, а тому ризик натрапити на чергових шахраїв теж достатньо високий). Однією з ознак такої шахрайської схеми є нижча ціна і легенда щодо спеціальних цін для потреб військових або закупівлі на сірому ринку тощо. З іншого боку, шахраї навпаки можуть завищувати ціну на продукцію, апелюючи до надвисокої якості продукції. Серед інших ознак волонтери називають невідповідність термінам поставок реальним термінам виготовлення продукції.

Шахрайські схеми від імені донаторів, благодійників та банків. За даними соціологічного дослідження «Громадянське суспільство в Україні в умовах війни – 2022», кількість зареєстрованих благодійних організацій в Україні за 2022 рік збільшилася майже у 8 разів (6 367 нових БО)¹⁷. Ці організації теж беруть участь у закупівлі необхідних речей для війська та українців, які постраждали від війни. До такого типу шахрайських схем належать такі, в яких шахраї справді переказують кошти на картку, часто кількома переказами невеликих сум. Саме цю інформацію зловмисники

¹⁶ Сітнікова, І. (2024), «Колишня «госпітальєрка» витратила донати на азартні ігри та подорожі. Що відомо про Адмірала Няв», Hromadske, 31 жовтня 2024. URL: <http://surl.li/vmfmbc> (дата звернення: 9.12.2024).

¹⁷ Громадянське суспільство в Україні в умовах війни (2023), Звіт за результатами дослідження, Київ, 64 с. URL: <http://surl.li/fywzkh> (останній перегляд 09 грудня 2024).

використовують для того, щоб від імені банківських установ телефонувати волонтерам і, посилаючись на фінансовий моніторинг і законодавство, вводити в оману щодо блокування збору, картки або рахунку на певний час. Також частина шахрайських схем відбувається через фейковий чат-бот у телеграмі. Такі чат-боти від імені банків часто мають синю пташку верифікації, проте таку мітку отримати у російському месенджері легко і це не є гарантією справжньої сторінки. Мета такої шахрайської схеми – підштовхнути волонтера до думки, що той має надати працівнику банку-шахраю доступ до рахунку.

Ця класифікація не остаточна, проте дає перелік основних шахрайських схем, пов'язаних із темою волонтерства.

Аналіз прикладів шахрайських схем за кожним із типів дає можливість виокремити дезінформаційні техніки, що використовуються у більшості медіаматеріалів, пов'язаних із волонтерством:

1. Підкріплення авторитетом. Найчастіше шахраї, для того, щоб отримати кошти, видають себе за тих, ким не є, використовують образ впізнаваних фондів, чужих імен, які мають добру репутацію у спільноті. Загалом імітують волонтерську діяльність і якась особа, і установа або ті, хто допомагає волонтерам та військовим.
2. Спільні цінності. За кожною шахрайською схемою, пов'язаною з волонтерством, стоять ті самі цінності: бажання допомогти, бажання перемоги, єдність суспільства, відчуття приналежності до спільноти. Найчастіше це внутрішня мотивація, яку використовують шахраї для того, щоб змусити людину переказати кошти.
3. Емоційність. У шахрайських схемах, пов'язаних зі зборами коштів та донатами, апелювання до емоцій – основне. Шахраї намагаються викликати емпатію у потенційної жертви, тому часто йдеться про порятунок життя, питання життя і смерті, життєво важливі потреби військових. У такий спосіб, а також за допомогою інших чинників, викликають гнів, страх, співчуття, жалість, радість та інші емоції.
4. Обмеження або затягування в часі. Залежно від типу шахрайської схеми, потенційну жертву шахраї ставлять в обмежений часовий слот, коли рішення потрібно прийняти в режимі «тут і зараз» (поки людина перебуває на емоціях і не здатна критично аналізувати ситуацію), або навпаки – затягують час. Найчастіше ця дезінформаційна техніка простежується у шахрайських схемах, що пов'язані з контрагентами та тими, у кого волонтери та фонди закуповують продукцію.
5. Вигадані історії. Як у фейках, так і в інформаційних операціях, в основі шахрайських схем – якісний і продуманий сторітелінг, який крок за кроком наштовхує людину на думку (а деколи навіть бажання) віддати кошти або передати особисті дані шахраям.
6. Підроблені профілі. Фейкові сторінки, фейкові відгуки як техніка у дезінформаційних кампаніях застосовується так само і у шахрайських схемах.

У 2022 р. збитки від шахрайства в інтернеті та з використанням методів соціальної інженерії (фактично з уведення в оману, щоб люди самостійно переказали

гроші) сягнули 1 млрд грн. У 2023 р. середня сума однієї шахрайської операції зросла на 49% – до 7900 грн¹⁸.

Зважаючи на типи шахрайств, пов'язаних із волонтерством, та на типи дезінформаційних технік, використаних у цих шахрайствах, важливим елементом у системі виявлення та протидії таким схемам є рекомендації, які розробила кіберполіція¹⁹:

1. Просити звіти за попередні періоди та збори;
2. Дізнатися більше про особу, зокрема, чи співпрацює вона з відомими організаціями чи публічними особами. У такому випадку на офіційних сторінках відповідних організацій та інфлюенсерів має також бути інформація про спільну діяльність;
3. Дізнатися, чи є нагороди, відзнаки за допомогу, відгуки про діяльність; чи висвітлена робота волонтера або приватної особи в інформаційному полі;
4. Скористатися сервісом пошуку зображень в Google для перевірки фотографій та скріншотів документів під збором – шахраї зазвичай використовують вкрадені чужі фото у своїх профілях;
5. Перевірити справжність посвідчення волонтера, зв'язавшись з організацією, яка видала документ;
6. Якщо йдеться про приватну особу, варто дізнатися, чому вона не зареєстрована як волонтер.

Наше дослідження дає змогу доповнити і розширити зазначені рекомендації, зважаючи саме на специфіку шахрайських схем, пов'язаних із волонтерством.

5. Результати і перспективи подальших досліджень обговорення.

Вивчення шахрайських схем, пов'язаних із волонтерством, що поширюються через медіа і залучають чимало людей, дає підстави запропонувати такі рекомендації щодо протидії дезінформації:

1. Детально проаналізувати персональні дані: назва сайту, доменне ім'я, дату створення сторінки чи профілю у соціальних мережах, а також пошукати сторінки та сайти-клони.
2. Перевірити назву фонду та звітність. Це можна зробити у системі YouControl або Opendatabot.
3. Вичерпно вивчити сайт та соціальні мережі фонду чи людини, яка збирає кошти (це може бути як військових, так і волонтер). Особливу увагу варто звернути на передісторію: як довго людина або організація займається волонтерством, як часто публікує звіти, чи справжні ці звіти, перевірити зображення та світлини за допомогою спеціалізованих сервісів.
4. Перевірити офіційні реквізити: кому належать, чи не фігурують зазначені картки як картки шахрайських зборів.
5. Не довіряти тим, хто збирає кошти на вулиці. Якщо це військові, то запитувати бригаду, переходити на сторінки бригади у соціальних мережах, запитувати, хто є керівником тощо і порівнювати інформацію з офіційною.

¹⁸ Opendatabot (2023), «Кількість справ про шахрайство зросла з початку 2023-го і перевищила показники за два попередні роки». URL: <http://surl.li/wdhpqe> (дата звернення: 9.12.2024).

¹⁹ Політковська, Ю. (2024), «У кіберполіції розповіли, як перевіряти волонтерів та благодійні організації, щоб не стати жертвою шахрайства», *detector.media*, 4 Березня 2024. URL: <http://surl.li/ptffac> (дата звернення: 9.12.2024).

6. Не поспішати. Якщо виникають найменші сумніви, то варто перевіряти діяльність або збір ретельніше.
7. Звертати увагу на помилки, друкує, імена, слова, які не притаманні українській мові. Це не завжди є ознакою шахрайства, але може бути одним з аспектів, які допоможуть не потрапити на гачок шахраїв.

Окремо варто розвивати на державному рівні цифрову та інфомедійну грамотність, щоб людина розуміла прийоми шахраїв і не ставала жертвою шахрайських схем.

У подальшому важливо апробувати і доповнити рекомендації щодо виявлення і протидії шахрайським схемам, що пов'язані із волонтерством. На особливу увагу заслуговує не тільки законодавче регулювання та притягнення до відповідальності, але й виявлення шахрайських схем, які пов'язані із розхитуванням інформаційної безпеки держави з боку Російської Федерації.

Вектором для обговорення та подальших досліджень є розширення типізації та опису шахрайських схем в умовах російсько-української війни відповідно до типів цільових аудиторій, на основі чутливих для українського суспільства питань, а також порівняння методів дезінформації, які використовують для шахрайства на темі волонтерства та інших типів шахрайств.

6. Висновки

У процесі дослідження медійних матеріалів щодо шахрайства на темі волонтерства ми класифікували типи шахрайських схем, основою яких є дезінформація. На основі теоретичних та практичних розвідок було виділено п'ять основних типів шахрайських схем, пов'язаних з волонтерством, серед яких шахрайства від імені військових, від імені благодійних фондів, від імені волонтерів, від контрагентів, які працюють із волонтерами та військовими, а також від імені донаторів та банківських установ. У шахрайських схемах використовують такі техніки дезінформації: апелювання до спільних цінностей, підкріплення авторитетом, створення вигаданих історій, емоційний тиск та маніпуляції часом.

Ми запропонували загальні рекомендації щодо виявлення та протидії шахрайським схемам, які включають як критичний підхід до аналізу інформації, так і фактчекерські алгоритми перевірки даних про фінансовий збір (незалежно від чийого імені збирають кошти). Окремим аспектом цих рекомендацій вказано розвиток цифрової та інфомедійної грамотності на рівні держави.

СПИСОК ЛІТЕРАТУРИ

1. Брисковська, О. М., Гелемей, М. О. (2023), «Особливості вчинення шахрайства в мережі інтернет в умовах воєнного стану», *Київський часопис права* (3), с. 174–180.
2. Вашкович, В. В., Василенко, О. Ю., Карабін, Т. О., Лазур, Я. В., Манзюк, В. В. та Рошканюк, В. М. (2022), *Посібник волонтера*, Видавничий дім «Гельветика», Одеса, 88 с. URL: <http://surl.li/fwtxgc> (останній перегляд 09 грудня 2024).
3. Громадянське суспільство в Україні в умовах війни (2023), Звіт за результатами дослідження, Київ, 64 с. URL: <http://surl.li/fywzkh> (останній перегляд 09 грудня 2024).

4. Закон України «Про благодійну діяльність та благодійні організації» (2024). URL: <https://zakon.rada.gov.ua/laws/show/5073-17#Text> (останній перегляд 09 грудня 2024).
5. Закон України «Про волонтерську діяльність» (2024). URL: <https://zakon.rada.gov.ua/laws/show/3236-17#Text> (останній перегляд 09 грудня 2024).
6. Кримінальний кодекс України (2024). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (останній перегляд 09 грудня 2024).
7. Левківська, Я. В. (2022), «Вплив воєнного стану на трансформувannya та розвиток інтернет-шахрайства в Україні», *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття*, т. 2, Видавничий дім «Гельветика», Одеса, с. 521–523.
8. Міжнародна організація міграції (2024), «Шахрайство, корупція та неправильне використання ресурсів». URL: <http://surl.li/ywuwqh> (останній перегляд 09 грудня 2024).
9. Павленко, Т. А. (2022), «Дезінформація: поняття, ознаки, перспективи протидії», *Юридичний науковий електронний журнал*, (7), с. 337–339.
10. Організації Північноатлантичного договору (2024), «Підхід НАТО у галузі боротьби з дезінформацією». URL: https://www.nato.int/cps/uk/natohq/topics_219728.htm (дата звернення: 9.12.2024).
11. Політковська, Ю. (2024), «У кіберполіції розповіли, як перевіряти волонтерів та благодійні організації, щоб не стати жертвою шахрайства», *detector.media*, 4 Березня 2024. URL: <http://surl.li/ptffac> (дата звернення: 9.12.2024).
12. Сітнікова, І. (2024), «Колишня «госпітальєрка» витратила донати на азартні ігри та подорожі. Що відомо про Адмірала Ная», *Нromadske*, 31 жовтня 2024. URL: <http://surl.li/vmfmhc> (дата звернення: 9.12.2024).
13. Чекмарьова, І. М. (2024), «Шахрайство в Інтернеті як один із видів шахрайства». *Аналітично-порівняльне правознавство*, Ужгород, 2, с. 639–643. URL: <http://surl.li/skxqxx> (останній перегляд 09 грудня 2024).
14. ACFE (2024) «Fraud 101: What Is Fraud?». URL: <http://surl.li/gnlas> (останній перегляд 09 грудня 2024).
15. Opendatabot (2023), «Кількість справ про шахрайство зросла з початку 2023-го і перевищила показники за два попередні роки». URL: <http://surl.li/wdhqze> (дата звернення: 9.12.2024).
16. Opendatabot (2024), «76% благодійних організацій не подають фінзвітність». URL: <https://opendatabot.ua/analytics/foundation-go-financial-reports> (дата звернення: 9.12.2024).
17. Opendatabot (2024), «Кожен дев'ятий опитаний українець ставав жертвою шахраїв від початку повномасштабного вторгнення». URL: <https://opendatabot.ua/analytics/stopfraud-nbu> (дата звернення: 9.12.2024).

REFERENCES

1. Bryskovska, O. M., & Helemei, M. O. (2023), Features of committing fraud on the Internet under martial law. *Kyiv Law Journal*, (3), 174–180.

2. Vashkovych, V. V., Vasylenko, O. Yu., Karabin, T. O., Lazur, Ya. V., Manziuk, V. V., & Roshkanyuk, V. M. (2022), *Posibnyk volontera* [Volunteer's Handbook]. Helvetika Publishing House, Odesa. URL: <http://surl.li/fwtxgc> (accessed 09, December, 2024).
3. Civil Society in Ukraine Under War Conditions – 2022. (2023). URL: <http://surl.li/fywzkh> (accessed 09, December, 2024).
4. Law of Ukraine on Charitable Activities and Charitable Organizations. (2024). URL: <https://zakon.rada.gov.ua/laws/show/5073-17#Text> (accessed 09, December, 2024).
5. Verkhovna Rada of Ukraine. (2024). *Law of Ukraine «On Volunteering»* (No. 3236-17). Official website of the Verkhovna Rada of Ukraine. URL : <https://zakon.rada.gov.ua/laws/show/3236-17#Text> (accessed 09, December, 2024).
6. Criminal Code of Ukraine. (2024). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (accessed 09, December, 2024).
7. Levkovska, Ya. V. (2022), The impact of martial law on the transformation and development of Internet fraud in Ukraine. In S. V. Kivalov (Ed.), *European choice of Ukraine, development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century* (Vol. 2, pp. 521-523). Helvetika Publishing House, Odesa.
8. International Organization for Migration. (2024). Fraud, corruption and misuse of resources. URL: <http://surl.li/ywuwHQ> (accessed 09, December, 2024).
9. Pavlenko, T. A. (2022), Disinformation: Concept, signs, prospects for counteraction. *Legal Scientific Electronic Journal*, 7, 337-339.
10. NATO approach to countering disinformation. (2024). URL: https://www.nato.int/cps/uk/natohq/topics_219728.htm (accessed 09, December, 2024).
11. Former ‘Hospitaller’ spent donations on gambling and travels: What is known about Admiral Nyav. (2024). URL: <http://surl.li/vmfmhC> (accessed December 9, 2024).
12. Cyberpolice told how to verify volunteers and charitable organizations to avoid becoming a victim of fraud. (2024). URL: <http://surl.li/ptffac> (accessed 09, December, 2024).
13. Chekmareva, I. M. (2024). Internet fraud as a type of fraud. *Analytical and Comparative Law*, 2024. URL: <http://surl.li/skxqxk> (accessed 09, December, 2024).
14. ACFE. (n.d.). Fraud 101: What Is Fraud? Available at URL: <http://surl.li/gnlas> (accessed 09, December, 2024).
15. Opendatabot. (2023). The number of fraud cases has increased since the beginning of 2023 and has exceeded the figures for the previous two years. URL <http://surl.li/wdhqze> (accessed 09, December, 2024).
16. Opendatabot (2024). 76% of charitable organizations do not submit financial reports. URL: <https://opendatabot.ua/analytics/foundation-go-financial-reports> (accessed 09, December, 2024).
17. Opendatabot. (2024). One in nine Ukrainians surveyed has been a victim of fraud since the full-scale invasion. URL: <https://opendatabot.ua/analytics/stopfraud-nbu> (accessed 09, December, 2024).

DISINFORMATION TECHNIQUES OF FRAUD ON THE TOPIC OF VOLUNTEERING DURING THE RUSSIAN-UKRAINIAN WAR

Alona Romaniuk

Educational and Research Institute of Journalism,

Taras Shevchenko National University of Kyiv

e-mail: aliona.romaniuk@knu.ua

<https://orcid.org/0009-0008-8127-8675>

Viktoriya Shevchenko

Educational and Research Institute of Journalism,

Taras Shevchenko National University of Kyiv

e-mail: victoryshe@knu.ua

<https://orcid.org/0000-0003-1642-1283>

This article examines disinformation techniques that underpin fraudulent schemes related to volunteering during the Russian-Ukrainian War. The research aims to classify fraudulent schemes exploiting disinformation in the context of volunteer activities and to develop recommendations for identifying signs of disinformation in pseudo-volunteer campaigns. Specific objectives include defining the concept of fraud and disinformation techniques, analyzing media mentions of volunteer fraud from 2022-2024, categorizing schemes based on the level of disinformation techniques, and proposing strategies to strengthen societal resilience to fraudulent influences.

The research employs a combination of bibliographic-semantic analysis to establish terminological consistency, content analysis of media reports, interviews with military volunteers, and systematic classification to identify types of fraudulent schemes. Data were collected from official resources such as Cyber Police, the National Bank of Ukraine, the Centre for Countering Disinformation, and fact-checking platforms. Primary data include interviews with 20 participants from the Volunteer Women's Summer School.

The study identifies five major types of fraudulent schemes linked to volunteering:

1. Fraud perpetrated in the name of «military personnel»
2. Schemes under the guise of charitable foundations.
3. Scams conducted in the name of individual volunteers.
4. Fraud by contractors collaborating with volunteers.
5. Schemes orchestrated by donors, benefactors, or banks.

Each category utilizes specific disinformation techniques, including emotional manipulation, appeals to shared values, fabricated stories, authority reinforcement, and time pressure.

The findings underscore the pervasive use of disinformation in fraudulent schemes targeting volunteer efforts. Recommendations to counteract such fraud include critical analysis of personal and organizational data, verification of reporting and financial transparency, and promoting digital and media literacy at a state level. This will enhance public awareness and resilience against scams.

Significance: The research contributes to the fields of information security and fraud prevention by addressing the intersection of disinformation and fraud in volunteering. It highlights the urgent need for systemic measures to safeguard volunteer activities, which are critical for societal solidarity and support during wartime. Moreover, the study's

recommendations have broader implications for combating fraud in other areas of public life, enhancing overall information security in Ukraine.

Keywords: Disinformation, online-fraud, Russian-Ukrainian War, information security, manipulation, online media, fraudulent schemes, medialiteracy.