DOI: 10.20535/2522-1078.2025.1(17).333979
ROR: 00syn5v21
УДК 004.056:316.77:327.5

Надходження до редакції: 13.03.2025
Прийняття до друку: 25.04.2025

Каменчук В. О.
аспірант кафедри видавничої справи та редагування Навчально-наукового видавничо-поліграфічного інституту, КПІ ім. Ігоря Сікорського, м. Київ, Україна
vadym.kamenchuk@gmail.com
ORCID: 0009-0004-4368-4366

Фіялка С. Б.
канд. наук із соц. комунікацій, доц. кафедри видавничої справи та редагування Навчально-наукового видавничо-поліграфічного інституту, КПІ ім. Ігоря Сікорського, м. Київ, Україна
fiialka.svitlana@lll.kpi.ua
ORCID: 0000-0002-1855-7574

Kamenchuk V.
postgraduate student of the Department of Publishing and Editing, Publishing and Printing Institutep of Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
vadym.kamenchuk@gmail.com
ORCID: 0009-0004-4368-4366

Fiialka S.
PhD in Social Communications, Associate Professor at the Department of Publishing and Editing, Educational and Scientific Publishing and Printing Institute, of Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
fiialka.svitlana@lll.kpi.ua
ORCID: 0000-0002-1855-7574

ПЕРСОНАЛЬНІ ДАНІ ЯК ІНСТРУМЕНТ ПРОПАГАНДИСТСЬКИХ КАМПАНІЙ: РИЗИКИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

PERSONAL DATA AS A TOOL OF PROPAGANDA CAMPAIGNS: RISKS TO INFORMATION SECURITY IN UKRAINE

Анотація. Досліджено актуальну проблему захисту персональних даних в Україні в умовах цифровізації. Соціальні мережі, месенджери, мобільні оператори, державні установи та бізнес-додатки збирають значні обсяги особистої інформації, включаючи демографічні дані, геолокацію, дані про купівельну поведінку, політичні вподобання, що дає змогу створювати детальні профілі користувачів. Персональні дані можуть бути використані як з рекламною метою, так і для цілеспрямованих пропагандистських кампаній.

Соціальні мережі, з огляду на широке охоплення аудиторії та технічні можливості для збирання аналітики дій користувачів, не лише виступають ключовим джерелом персональних даних, а й становлять високий потенційний ризик через можливість їх використання для маніпулятивного впливу на користувачів, що може мати глибокі соціальні та політичні наслідки. Месенджери, такі як Telegram, становлять ризик через недостатній рівень контролю над зберіганням даних. Аналіз діяльності мобільних операторів демонструє їхню здатність збирати детальну поведінкову

інформацію, включаючи локаційні дані та фінансові транзакції, що збільшує ризики для фізичної безпеки та підвищує загрози шахрайських дій. Державні установи, що пропонують цифрові послуги, накопичують значний обсяг персональної інформації, але стикаються з проблемами кіберзахисту, що може призвести до незаконного доступу до персональних даних громадян. Бізнес-додатки, такі як маркетплейси чи сервіси таксі, збирають дані для оптимізації сервісів і таргетованої реклами, що також створює ризики зловживання персональними даними, витоків інформації та маніпулювання поведінкою користувачів.

Рівень захисту персональних даних в Україні залишається недостатнім. Це створює передумови для поширення персоналізованої пропаганди та інших форм маніпуляції. Автори наголошують на необхідності посилення кіберзахисту, запровадження прозорих стандартів оброблення даних та підвищення обізнаності громадян про важливість збереження їхньої приватності. Особливу увагу приділено викликам, пов'язаним з доступом до великих масивів даних та їх використанням для створення таргетованих інформаційних кампаній. Запропоновано рекомендації для мінімізації ризиків, пов'язаних з використанням персональних даних, та підвищення рівня інформаційної безпеки в країні.

Ключові слова: персональні дані, персоналізована пропаганда, соціальні мережі, мобільні оператори, державні установи, кіберзахист, профіліювання, мікротаргетування.

Abstract. The study examines the pressing issue of personal data protection in Ukraine within the context of digitalization. Social networks, messaging applications, mobile operators, government institutions, and business applications collect substantial amounts of personal information, including demographic data, geolocation, purchasing behavior, and political preferences, enabling the creation of detailed user profiles. Personal data can be utilized not only for advertising purposes but also for targeted propaganda campaigns.

Social media, due to their extensive audience reach and technical capabilities for collecting user activity analytics, serve not only as a primary source of personal data but also pose a significant potential risk due to their capacity for manipulative influence on users, which may have profound social and political consequences. Messaging applications, such as Telegram, present risks due to the insufficient level of control over data storage. The analysis of mobile operators' activities demonstrates their ability to collect detailed behavioral information, including location data and financial transactions, which increases risks to physical security and heightens the threat of fraudulent activities. Government institutions that provide digital services accumulate vast amounts of personal information yet face cybersecurity challenges that may lead to unauthorized access to citizens' personal data. Business applications, such as marketplaces and taxi services, collect data to optimize services and enable targeted advertising, which also creates risks of personal data misuse, information leaks, and behavioral manipulation of users.

The level of personal data protection in Ukraine remains insufficient. This creates favorable conditions for the spread of personalized propaganda and other forms of manipulation. The authors emphasize the need to strengthen cybersecurity measures, implement transparent data processing standards, and enhance citizens' awareness of the importance of privacy protection. Special attention is given to challenges related to access to large datasets and the use of artificial intelligence for designing targeted information campaigns. The study proposes recommendations for minimizing risks associated with personal data usage and improving the overall level of information security in the country.

Keywords: personal data, personalized propaganda, social networks, mobile operators, government institutions, cybersecurity, profiling, microtargeting.

Вступ. Персоналізовані пропагандистські кампанії — це новітній інструмент впливу, що змінює інформаційний ландшафт і формує громадську думку, особливо в умовах зростання технологічних можливостей. Поширення персоналізованої пропаганди та значне збільшення обсягів збору персональних даних, зокрема комерційними та державними компаніями, створює нові ризики для інформаційної безпеки, і передусім у контексті російської інформаційної війни проти України.

Використання персональних даних для підготовки пропагандистських кампаній суттєво підвищує їх ефективність. Одним з перших промовистих випадків такої пропаганди була кампанія консалтингової фірми Cambridge Analytica, коли збирання даних через фейсбук-додаток thisisyourdigitallife дало змогу створювати на основі лайків та інших поведінкових характеристик психологічні портрети користувачів [4]. Було використано інструмент профілювання OCEAN, що розділяв профілі за п'ятьма параметрами — Openness (відкритість), Conscientiousness (сумлінність), Extraversion (екстраверсія), Agreeableness (здатність до погодження) та Neuroticism (невротизм) [10]. Це дозволило сегментувати аудиторію та налаштовувати таргетовані повідомлення для користувачів, здатних коливатися в політичних уподобаннях, і, таким чином, схилити голосувати за потрібного кандидата на виборах президента США 2016 р. Цей метод дістав назву «мікротаргетування» — тип персоналізованої комунікації, який передбачає збирання персональних даних про людей, відповідне сегментування аудиторії та використання цієї інформації для показу цільової політичної реклами [21].

Досвід Cambridge Analytica свідчить про потужний вплив мікротаргетування. Переваги таргетованих персоналізованих пропагандистських

кампаній перед класичними підтверджують і незалежні експериментальні дослідження, які показують в окремих випадках на 70 % більшу ефективність [17]. Окремою проблемою є виявлення замовників таких кампаній, а іноді й самого факту впливу через їхню високоточну та приховану природу, адже, на відміну від класичних методів, у разі використання мікротаргетування пропагандистські повідомлення отримує тільки обмежене коло користувачів [16].

Наразі дослідники фіксують застосування таргетованої політичної реклами, що базується на персональних даних, через соціальні мережі в 95 країнах під час 113 національних виборів [18]. Ці випадки не залишилися поза увагою громадськості та державних органів. Зокрема, компанію Meta було притягнуто до суду, а її засновник Марк Цукерберг надавав свідчення перед Сенатом США. У відповідь на це у 2018 р. великі платформи, такі як Google, Facebook і Twitter, запровадили відкриті архіви політичної реклами для забезпечення прозорості [14]. Європейський Союз також посилив регламент захисту персональних даних (GDPR). Проте, за оцінками дослідників, чинні норми все ще не забезпечують достатнього захисту від мікротаргетування та профілювання [5].

Збір персональних даних є обов'язковою умовою для ефективного мікротаргетування. Психологічне профілювання, на кшталт того, яке застосовувала Cambridge Analytica, стає дедалі точнішим і дозволяє ефективніше досягати цільових аудиторій, зокрема, завдяки зібраним персональним даним українців. Дослідження показують, що громадяни часто недооцінюють значення персональних даних, вважаючи себе не вразливими до впливу [11].

Ефект персоналізованої пропаганди підсилюється, коли користувачі самі поширюють дезінформацію в соціальних мережах та месенджерах. Чимало людей, отримуючи маніпулятивні чи фейкові повідомлення від знайомих чи близьких, свідомо уникають спростувань, оскільки прагнуть не конфліктувати з друзями та родичами [6]. Така пасивність призводить до подальшого поширення неправдивих меседжів, адже користувач, що поширив його і не отримав спростування, сприймає мовчання як підтвердження.

У контексті персоналізованої пропаганди, незважаючи на активні контрдії України масованим пропагандистським кампаніям з боку Росії, ефективно протидіяти мікротаргетованим кампаніям значно складніше.

Мета статті — оцінити ризики, пов'язані з впливом персоналізованої пропаганди в Україні, з акцентом на оцінюванні кількості та якості персональних даних, що акумулюються комерційними компаніями та державними установами. У межах дослідження розглянуто суб'єкти, які накопичують персональну інформацію, визначено й класифіковано типи даних, які збираються, та проаналізовано ризики їх використання для створення персоналізованих пропагандистських кампаній, що можуть впливати на інформаційну безпеку.

Методи дослідження. У дослідженні використано порівняльний аналіз для оцінювання відмінностей у зборі та використанні персональних даних, що дозволило визначити рівень ризиків їх застосування в пропагандистських кампаніях.

Було здійснено контент-аналіз персональних даних, що збираються соціальними мережами, месенджерами, мобільними операторами, державними установами та бізнес-додатками. Спершу визначено вибірку досліджуваних матеріалів, що охоплювала інформацію про обсяги та типи зібраних даних. Далі проведено аналіз кількості та якості цих даних з точки зору їхньої придатності для профілювання користувачів. Завершальним етапом стала оцінка ризиків використання отриманих персональних даних у пропагандистських кампаніях, з урахуванням їхньої доступності, а також зафіксованих чи потенційних випадків їх використання в інформаційних операціях.

Емпіричний аналіз відкритих даних про зібрані персональні дані українських громадян дозволив провести класифікації типів персональних даних.

Результати проведених досліджень. Матеріалом дослідження стали ключові накопичувачі персональних даних українських громадян з характеристиками їхньої діяльності та типами інформації, яку вони збирають. Розглянуто соціальні мережі, месенджери, мобільні оператори, державні установи та бізнес-сервіси.

Соціальні мережі. Соціальні мережі, зокрема Facebook, Instagram, X/Twitter, YouTube та TikTok, є потужними джерелами персональних даних, придатними для профілювання та поширення персоналізованої пропаганди [19]. Було зафіксовано численні випадки їх залучення до таких процесів, переважно в контексті президентських та проміжних виборів у США, а також виборчих кампаній в Австралії, Канаді, Нідерландах, Великобританії, Іспанії та Німеччині [18].

Соціальні мережі збирають такі демографічні дані, як вік, стать, місце проживання, освіта, професія та сімейний стан. Їх зазвичай уписують добровільно під час реєстрації або заповнення профілю, але ці дані можна також отримати через аналіз поведінки користувача.

Проте найбільшу цінність для профілювання становить поведінкова інформація — дані, що відображають активність і звички користувача під час взаємодії з контентом. Соціальні мережі відстежують, які публікації вподобані або прокоментовані, які відео переглянуто повністю, а які закрито через кілька секунд. Фіксується, на яких дописах користувач зупиняється довше, які статті відкриває та читає, а які лише переглядає в стрічці новин. Навіть темп прокручування сторінки може свідчити про рівень зацікавленості тією чи іншою темою [20].

Політичні вподобання виявляються через підписки на авторів і сторінки, участь у політичних або соціальних групах, а також через коментарі та реакції на новини. У деяких випадках соцмережі аналізують навіть тональність висловлювань користувача, що дає змогу визначити його ставлення до певних питань. Такі дані є особливо цінними для цільової сегментації аудиторій, персоналізації рекламних кампаній та інформаційних впливів, зокрема пропагандистських [20].

Крім цього, відстежуються технічні параметри використання соцмереж: тип пристрою, операційна система, IP-адреса, геолокація, а також звички користувача щодо підключення до Wi-Fi або мобільних мереж. Це дозволяє не лише показувати контент відповідно до місцезнаходження, а й визначати, де і коли людина найбільш активна в онлайні.

Завдяки такому комплексному збору даних соціальні мережі отримують надзвичайно точне уявлення про поведінку, вподобання та навіть емоційний стан користувачів. Це створює широкі можливості як для маркетингу, так і для маніпулятивного впливу, зокрема через персоналізовані інформаційні кампанії [19].

Самі платформи пропонують своїм клієнтам на комерційній основі широкі можливості масованої таргетованої реклами, використовуючи наявні профілі користувачів. Попри відкриття архівів замовлень політичної реклами після серії скандалів, це лише частково підвищило прозорість процесів і забезпечило кращі можливості для моніторингу [14].

Нижче подано зведену таблицю з порівнянням соціальних мереж за кількістю та якістю персональних даних користувачів (табл. 1).

Таблиця 1

Персональні дані, що збираються соціальними мережами

Мережа	Кількість даних	Типи даних	Якість даних
Facebook	Велика (широкий спектр персональної інформації, що дозволяє створювати глибокі профілі користувачів)	Основна інформація (ім'я, вік, стать, контакти) Локаційні дані Дії на платформі (уподобання, коментарі, пошук, кліки) Поведінкові дані (перегляди сторінок, мережа друзів, активність у групах) Дані з інших сайтів через Facebook Pixel Файли cookie та дані пристрою	Висока — Facebook збирає як структуровані (реєстраційні) дані, так і неструктуровані (поведінкові, мережеві зв'язки), що дає змогу формувати детальні профілі користувачів [19, с. 122646]
Instagram	Велика (візуальний контент, соціальні взаємодії, геолокація та активність користувача)	Основна інформація (як у Facebook) Візуальний контент (фото, відео, історії) Геолокація Дані про взаємодію з контентом (реакції, коментарі, збереження, репости) Дані про рекламні вподобання	Висока — Instagram фокусується на візуальних даних та взаємодіях користувачів із контентом, що дозволяє аналізувати їхні інтереси та емоційні реакції [19, с. 122643]
X (Twitter)	Середня (текстові взаємодії, мережеві інтереси, однак менше персональної інформації порівняно з Facebook чи Instagram)	Основна інформація (ім'я, нікнейм, контактні дані) Історія твітів, ретвітів, лайків Геолокація (за згодою) Дані про пристрої та браузери Мережеві зв'язки (з ким взаємодіє користувач)	Середня — X зберігає багато текстової інформації, значна частина даних є публічною [19, с. 122646]
YouTube	Велика (інформація, що дає змогу формувати детальні рекомендації та впливати на інформаційне середовище користувача)	Історія переглядів і пошуку Уподобання, коментарі, підписки Дані про пристрої, браузери та мережу Час перегляду та інтереси Геолокація	Висока — YouTube формує глибокі профілі на основі історії переглядів, що дає змогу прогнозувати інтереси користувача [9]
TikTok	Велика (велика кількість даних для подальшого використання алгоритмів поведінкового аналізу)	Основна інформація Відеовзаємодії (перегляди, лайки, коментарі, збереження) Геолокація Біометричні дані Дані про пристрої та мережу	Дуже висока — TikTok аналізує поведінку користувачів детальніше, ніж інші платформи, особливо у сфері відеоінтеракцій, що дозволяє створювати надзвичайно точні алгоритми персоналізації [22, с. 18]

Водночас персоналізовані кампанії ґрунтуються не лише на інформації, зібраній безпосередньо в соціальних мережах, а й на даних з інших джерел, що дає змогу створювати більш деталізовані профілі користувачів та посилювати ефективність таргетованих впливів. Хоча наявні емпіричні дослідження в основному фіксують використання даних соціальних мереж для мікротаргетованої пропаганди, існують серйозні ризики залучення інших джерел збору персональних даних, зокрема державних реєстрів, баз даних мобільних операторів, комерційних сервісів та маркетингових платформ. Приклад виборів у Кенії 2013 р. демонструє, що Cambridge Analytica використовувала не лише дані з Facebook, а й інформацію з публічних баз виборців, що дало змогу сегментувати аудиторію за соціально-демографічними характеристиками та ідеологічними переконаннями [12]. Це вказує на можливість подальшого розширення практики використання персональних даних поза межами соціальних мереж, що потребує ретельного дослідження з огляду на загрози для інформаційної безпеки та демократичних процесів.

Мобільні оператори. Мобільні оператори відіграють значну роль у збиранні та обробленні персональних і поведінкових даних своїх користувачів. Ці компанії щодня отримують інформацію про місцеположення абонентів у реальному часі, їхні активності, звички, телефонні дзвінки, обмін повідомленнями, а також фінансові транзакції. Абоненти часто не усвідомлюють, наскільки детальні дані про їхнє життя акумулюються й аналізуються.

Завдяки розвитку технологій Big Data мобільні оператори надають доступ до своєї аналітики комерційним клієнтам. Таку інформацію широко використовують для маркетингових, логістичних і соціальних досліджень [8], але також може бути ризик зловживань.

Кіберзагрози є ще одним аспектом, який підкреслює важливість захисту даних. Наприклад, кібератаки на мережі провідних операторів, таких як «Київстар», призводили до серйозних наслідків, включно з потенційним витоком великих обсягів інформації [2]. Такі дані, якщо потраплять до рук зловмисників, можуть використовуватися у пропагандистських кампаніях.

Основні категорії даних, що їх збирають мобільні оператори: телефонні номери, демографічні дані (вік, стать, адреса, місце роботи, особливо для контрактних абонентів), поведінкові дані (дані про локації, маршрути переміщення, історію дзвінків і повідомлень, а також фінансові транзакції).

Месенджери. Найбільш популярними месенджерами в Україні є Telegram, Viber, WhatsApp. З початком повномасштабного вторгнення найбільшу увагу привертає Telegram, адже ця платформа стала популярним джерелом новин, де багато українців шукають оперативну та достовірну інформацію. Він отримав високу довіру серед українських користувачів, що робить його особливо привабливим для поширення інформації [7]. Численні дослідження підтверджують використання месенджера Telegram для поширення пропаганди та збору персональних даних. Наприклад, згідно з аналізом Центру стратегічних комунікацій та інформаційної безпеки, у 2019–2021 рр. на Telegram-каналі «НачШтабу» було зафіксовано 131 повідомлення, які містили заклики до збору, а також публікацію персональних даних, зокрема чутливої військової інформації, документів або їх проєктів [3].

Перелік підписок на канали дозволяє формувати детальні профілі користувачів, зокрема їхні політичні вподобання. Зловмисники, маючи доступ до баз налаштувань користувачів або використовуючи прив'язку до мобільних номерів, можуть створювати інформаційні кампанії, таргетовані на конкретні групи. Такі кампанії можуть проводитись як у Telegram, так і через інші соціальні мережі, що розширює їхній вплив. Особливо небезпечним є ризик втручання через потенційний доступ до баз даних спецслужбами Росії, ураховуючи походження засновника Telegram Павла Дурова [15].

Окрім цього, дані збираються через боти, які поширюють популярні патерни контенту, залучаючи користувачів до таргетованих груп [13]. Невидимість таких процесів для більшості користувачів та довіра до платформи значно ускладнюють виявлення й протидію загрозам. Це робить месенджери (зокрема Telegram) потужними інструментами персоналізованої пропаганди та викликом для інформаційної безпеки України.

Державні установи. Україна демонструє значний прогрес у цифровізації державних послуг, що забезпечує зручність для громадян і підвищує ефективність управління. Зокрема, платформи Дія, ЕСОЗ та Резерв+ стали ключовими інструментами збирання та оброблення персональних даних.

Однак цифровізація також несе суттєві ризики. Існує ймовірність витоків даних, зважаючи на їх високий обсяг і чутливість, і такі випадки вже мали місце, наприклад кібератака на державні реєстри України, що відбулася 19 грудня 2024 р., унаслідок якої близько 60 різних державних реєстрів виявились недоступними [1]. Зростання кількості

користувачів державних цифрових платформ підвищує масштаби таких ризиків.

Основні категорії персональних даних, що акумулюються: телефонний номер, демографічна інформація (ім'я, вік, стать, сімейний стан, адреса проживання тощо), специфічні дані та документи (паспорти, паспортні дані, медичні записи, фінансові документи, результати тестів і скан-копії офіційних документів).

Необхідність посилення захисту таких баз даних є критично важливою для запобігання зловживанням і підвищення інформаційної безпеки держави.

Бізнес-сервіси. Ринок Big Data активно стимулює розвиток нових підходів до збирання та використання персональних даних у різних галузях. В Україні бізнес-платформи, зокрема ритейл-компанії (Rozetka, OLX, Prom.ua, Hotline), використовують ці дані для формування детальних профілів клієнтів. Це сприяє підвищенню ефективності персоналізованої реклами та створює умови для оптимізації маркетингових кампаній.

Інші сектори, наприклад сервіси таксі (Uklon, Uber, Bolt), акумулюють геодані, які дозволяють проводити поведінковий аналіз. Це відкриває можливості для створення нових каналів таргетованого впливу, зокрема інформаційних.

Основні категорії даних, що збираються: контактна інформація (телефонні номери, адреси електронної пошти), демографічні відомості (адреси проживання та інші дані), поведінкові характеристики (купівельні звички, частота використання послуг, динамічні геолокаційні дані).

Зростання обсягів накопичення цих даних підвищує ризики витоків і зловживання, особливо в умовах браку жорсткого регулювання обробки такої інформації.

Нижче наведено зведену таблицю класифікації персональних даних, що збираються з оцінками ризиків використання персональних даних у мікротаргетованих пропагандистських кампаніях (табл. 2). Визначені такі рівні ризиків:

Високий ризик — дані містять демографічну, поведінкову, фінансову та політичну інформацію, що дає змогу створювати точні профілі користувачів. Низький рівень захисту та доведене використання в пропаганді (наприклад, соціальні мережі) підвищують загрозу маніпуляції суспільною думкою.

Середній ризик — обсяг зібраних даних обмежений, але можливе профілювання через непрямі характеристики (наприклад, державні

установи). Використання для пропаганди здебільшого опосередковане та залежить від витоків даних.

Низький ризик — збір мінімального набору технічних або анонімних даних, що не дозволяє точно ідентифікувати користувачів. Брак механізмів маніпуляції робить ці дані малопридатними для пропагандистських кампаній (наприклад, мобільні оператори та бізнес-додатки).

Таблиця 2

Зведена таблиця типів персональних даних, що збираються

Накопичувач	Телефон	Демографічні дані	Полі-тичні вподобання	Пове-дінкові, психологічні	Оцінка ризиків використання у мікротаргетованих пропагандистських кампаніях
Соцмережі (Facebook, Instagram, X/ Twitter, YouTube)	Так	Так	Так	Так	Рівень ризику: високий. Соцмережі є основним майданчиком для мікротаргетованих інформаційних кампаній, оскільки надають детальні дані про користувачів та забезпечують високоточне таргетування. Відомі випадки їх використання в політичних та пропагандистських кампаніях (наприклад, Cambridge Analytica) 11]
Месенджери (Telegram, Viber, WhatsApp)	Так	Ні	Так	Ні	Рівень ризику: високий. Месенджери стають ключовими платформами для поширення дезінформації та маніпулятивного контенту, особливо серед уже сформованих аудиторій. Найбільші ризики пов'язані з використанням Telegram, який активно застосовується для інформаційних атак [13]
Мобільні оператори	Так	Так	Ні	Так	Рівень ризику: низький. Дані мобільних операторів можуть бути використані для відстеження руху певних груп населення, аналізу соціальних зв'язків та створення моделей поведінки. Вони менш ефективні для прямого таргетування, але можуть доповнювати інші джерела інформації
Державні установи	Так	Так	Ні	Ні	Рівень ризику: середній. Державні дані можуть не лише бути основою для створення персоналізованих загроз, шантажу та дискредитаційних кампаній, але й доповнювати мікротаргетовані кампанії [12]
Бізнес-додатки	Так	Ні	Ні	Так	Рівень ризику: низький. Хоча дані бізнес-додатків не є основним джерелом для мікротаргетування, вони можуть допомагати у формуванні загальної картини про користувача. У комбінації з іншими джерелами (соцмережами, мобільними операторами) вони можуть підвищувати ефективність пропагандистських кампаній

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Несенюк А., Мельник Т., Балашова Л. «За атакою стоять російські спецслужби». Понад 60 держреєстрів не працюють через кібератаку росіян на Мін'юст. Які наслідки й чим загрожує українцям потенційний витік даних. Forbes Ukraine. 20 грудня 2024. URL: https://forbes.ua/innovations/za-atakoyu-stoyat-rosiyski-spetssluzhbi-ponad-60-derzhreestriv-ne-pratsyuyut-cherez-ataku-rosiyan-na-minyust-yaki-naslidki-y-chim-zagrozhue-ukraintsyam-vitik-danikh-20122024-25742 (дата звернення: 22.12.2024).
2. Тарасовський Ю. Хакери перебували в системі «Київстару» з травня 2023 року. СБУ розкрила деталі кібератаки. Forbes Ukraine. 2024, 4 січня. URL: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307 (дата звернення: 22.12.2024).
3. Центр стратегічних комунікацій. «НачШтабу»: Аналітична записка по Telegram-каналу. 2024, 17 вересня. URL: https://spravdi.gov.ua/telegram-kanal-nachshtabu/ (дата звернення 05.02.2025).
4. Berghel H. Malice Domestic: The Cambridge Analytica Dystopia. Computer. 2018, May 24. Vol. 51(5). Pp. 84–89. https://doi.org/10.1109/MC.2018.2381135.
5. Blasi Casagran C., Vermeulen M. Reflections on the murky legal practices of political micro-targeting from a GDPR perspective. International Data Privacy Law. 2021, November. Vol. 11(4). Pp. 348–359. https://doi.org/10.1093/idpl/ipab018.
6. Chadwick A., Vaccari C., Hall N. What Explains the Spread of Misinformation in Online Personal Messaging Networks? Exploring the Role of Conflict Avoidance. Digital Journalism. 2023, May 10. Vol. 12(5). Pp. 574–593. https://doi.org/10.1080/21670811.2023.2206038.
7. Denisova K. Is Telegram, Ukraine's most popular messenger app, a Russian Trojan horse? The Kyiv Independent. 2024, August 28. URL: https://kyivindependent.com/is-ukraines-most-popular-messenger-app-a-russian-trojan-horse/ (accessed on 01.02.2025)
8. Halan O., Skoromnyi V., Pustovit N. Big data technologies application in the activities of modern enterprises. Norwegian Journal of development of the International Science. 2022, October 26. No 95. Pp. 64–68. https://doi.org/10.5281/zenodo.7258922.
9. Haroon M., Chhabra A., Liu X., Mohapatra P., Shafiq Z., Wojcieszak M. YouTube, The Great Radicalizer? Auditing and Mitigating Ideological

Biases in YouTube Recommendations. 2022. arXiv:2203.10666 [cs.CY]. https://doi.org/10.48550/arXiv.2203.10666.
10. Heawood J. Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. Information Polity. 2018, November. Vol. 23(4). Pp. 429–434. https://doi.org/10.3233/IP-180009.
11. Hinds J., Williams E., Joinson A. „It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies. 2020, November. Vol. 143. https://doi.org/10.1016/j.ijhcs.2020.102498.
12. Kitili J. What is Political Microtargeting and what are the risks involved? The Centre for Intellectual Property and Information Technology Law (CIPIT). 2022, August 5. URL: https://cipit.strathmore.edu/what-is-political-microtargeting-and-what-are-the-risks-involved/ (accessed on 24.02.2025).
13. La Morgia M., Mei A., Mongardini A., and Wu J. Uncovering the Dark Side of Telegram: Fakes, Clones, Scams, and Conspiracy Movements. 2021, November 29. arXiv:2111.13530 [cs.CY]. https://doi.org/10.48550/arXiv.2111.13530.
14. Leerssen P., Ausloos J., Zarouali B., Helberger N., de Vreese C. Platform ad archives: promises and pitfalls. Internet Policy Review. 2019, October 9. Vol. 8(4). https://doi.org/10.14763/2019.4.1421.
15. Marechal N. From Russia With Crypto: A Political History of Telegram. 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18). 2018. URL: https://www.usenix.org/system/files/conference/foci18/foci18-paper-marchal.pdf (accessed on 14.12.2024)
16. Ó Fathaigh R., Dobber T., Zuiderveen Borgesius F., Shires J. Microtargeted propaganda by foreign actors: An interdisciplinary exploration. Maastricht Journal of European and Comparative Law. 2021, November 16. Vol. 28(6). Pp. 856–877. https://doi.org/10.1177/1023263X211042471.
17. Tappin B., Wittenberg C., Hewitt L., Rand D. Quantifying the potential persuasive returns to political microtargeting. PNAS. 2023, May 7. Vol. 120(25). https://doi.org/10.1073/pnas.2216261120.
18. Votta F., Kruschinski S., Hove M., Helberger N., Dobber T., de Vreese C. Who Does(n't) Target You? Mapping the Worldwide Usage of Online Political Microtargeting. JQD:DM. 2024, May 1. Vol. 4. Pp. 1–73. https://doi.org/10.51685/jqd.2024.010.
19. Wu W., Ghazali M., Hazlin Huspi S. A Review of User Profiling Based on Social Networks. IEEE Access. 2024, July 19. Vol. 12. Pp. 122642–122670. https://doi.org/10.1109/ACCESS.2024.3430987.

20. Zarouali B., Dobber T., De Pauw G., de Vreese C. Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. Communication Research. 2022, December. Vol. 49(8). Pp. 1066–1091. https://doi.org/10.1177/0093650220961965.
21. Zuiderveen Borgesius F., Möller J., Kruikemeier S., Ó Fathaigh R., Irion K., Dobber T., Bodo B., de Vreese C. Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review. 2018, February 9. Vol. 14(1). Pp. 82–96. https://doi.org/10.18352/ulr.420.
22. Zoroayka V., Lingelbach K., Rigole N. Privacy, security, and awareness perceptions on the use of social media: a TikTok focus. Issues In Information Systems. 2023. Vol. 24(4). Pp. 16–24. https://doi.org/10.48009/4_iis_2023_102.

REFERENCES

1. Nesenyuk, A., Melnyk, T., & Balashova, L. (2024). „Za atakoyu stoyat rosiyski spetssluzby". Ponad 60 derzhreyestriv ne pratsyuyut cherez kiberataku rosiyan na Minjust. Yaki naslidky j chym zagrozhuye ukrayyintsyam potentsiynyy vytik danyh. [„Russian special services are behind the attack". Over 60 state registries are out of service due to Russian cyberattack on the Ministry of Justice. What are the consequences and threats to Ukrainians from a potential data leak]. Forbes Ukraine. Retrieved 22 December 2024 from https://forbes.ua/innovations/za-atakoyu-stoyat-rosiyski-spetssluzhbi-ponad-60-derzhreestriv-ne-pratsyuyut-cherez-ataku-rosiyan-na-minyust-yaki-naslidki-y-chim-zagrozhue-ukraintsyam-vitik-danikh-20122024-2574.
2. Tarasovskyi, Y. (2024). Hakery perebuvaly v systemi „Kyivstaru" z travnya 2023 roku. SBU rozkryla detail kiberataky [Hackers were in Kyivstar's system since May 2023. SBU revealed details of cyberattack]. Forbes Ukraine. Retrieved 22 December 2024 from https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307.
3. Tsentr stratehichnykh komunikatsii (2024). „NachShtabu": Analitychna zapyska po Telegram-kanalu [„NachShtabu": Analytical note on the Telegram channel]. Spravdi. Retrieved 5 February 2025 from https://spravdi.gov.ua/telegram-kanal-nachshtabu/.
4. Berghel, H. (2018). Malice domestic: The Cambridge Analytica dystopia. Computer, 51(5), 84–89. https://doi.org/10.1109/MC.2018.2381135.

5. Blasi Casagran, C., & Vermeulen, M. (2021). Reflections on the murky legal practices of political micro-targeting from a GDPR perspective. International Data Privacy Law, 11(4), 348–359. https://doi.org/10.1093/idpl/ipab018.
6. Chadwick, A., Vaccari, C., & Hall, N. A. (2023). What Explains the Spread of Misinformation in Online Personal Messaging Networks? Exploring the Role of Conflict Avoidance. Digital Journalism, 12(5), 574–593. https://doi.org/10.1080/21670811.2023.2206038.
7. Denisova, K. (2024). Is Telegram, Ukraine's most popular messenger app, a Russian Trojan horse? The Kyiv Independent. Retrieved 15 December 2024 from https://kyivindependent.com/is-ukraines-most-popular-messenger-app-a-russian-trojan-horse/.
8. Halan, O., Skoromnyi, V., & Pustovit, N. (2022). Big data technologies application in the activities of modern enterprises. Norwegian Journal of Development of the International Science, 95, 64–68. https://doi.org/10.5281/zenodo.7258922.
9. Haroon, M., Chhabra, A., Liu, X., Mohapatra, P., Shafiq, Z., & Wojcieszak, M. (2022). YouTube, the great radicalizer? Auditing and mitigating ideological biases in YouTube recommendations. arXiv:2203.10666 [cs.CY]. https://doi.org/10.48550/arXiv.2203.10666.
10. Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. Information Polity, 23(4), 429–434. https://doi.org/10.3233/IP-180009.
11. Hinds, J., Williams, E., & Joinson, A. (2020). „It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 143, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498.
12. Kitili, J. (2022). What is political microtargeting and what are the risks involved? The Centre for Intellectual Property and Information Technology Law (CIPIT). Retrieved February 8, 2025, from https://cipit.strathmore.edu/what-is-political-microtargeting-and-what-are-the-risks-involved/.
13. La Morgia, M., Mei, A., Mongardini, A., & Wu, J. (2021). Uncovering the dark side of Telegram: Fakes, clones, scams, and conspiracy movements. arXiv:2111.13530 [cs.CY]. https://doi.org/10.48550/arXiv.2111.13530
14. Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., & de Vreese, C. (2019). Platform ad archives: Promises and pitfalls. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1421.

15. Marechal, N. (2018). From Russia with crypto: A political history of Telegram. 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18). Retrieved 18 December 2024 from https://www.usenix.org/system/files/conference/foci18/foci18-paper-marchal.pdf.
16. Ó Fathaigh, R., Dobber, T., Zuiderveen Borgesius, F., & Shires, J. (2021). Microtargeted propaganda by foreign actors: An interdisciplinary exploration. Maastricht Journal of European and Comparative Law, 28(6), 856–877. https://doi.org/10.1177/1023263X211042471.
17. Tappin, B., Wittenberg, C., Hewitt, L., & Rand, D. (2023). Quantifying the potential persuasive returns to political microtargeting. PNAS, 120(25). https://doi.org/10.1073/pnas.2216261120.
18. Votta, F., Kruschinski, S., Hove, M., Helberger, N., Dobber, T., & de Vreese, C. (2024). Who does(n't) target you? Mapping the worldwide usage of online political microtargeting. Journal of Quantitative Description: Digital Media, 4, 1–73. https://doi.org/10.51685/jqd.2024.010.
19. Wu, W., Ghazali, M., & Hazlin Huspi, S. (2024). A review of user profiling based on social networks. IEEE Access, 12, 122642–122670. https://doi.org/10.1109/ACCESS.2024.3430987.
20. Zarouali, B., Dobber, T., De Pauw, G., & de Vreese, C. (2022). Using a personality-profiling algorithm to investigate political microtargeting: Assessing the persuasion effects of personality-tailored ads on social media. Communication Research, 49(8), 1066–1091. https://doi.org/10.1177/0093650220961965.
21. Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. Utrecht Law Review, 14(1), 82–96. https://doi.org/10.18352/ulr.420.
22. Zoroayka, V., Lingelbach, K., & Rigole, N. (2023). Privacy, security, and awareness perceptions on the use of social media: A TikTok focus. Issues in Information Systems, 24(4), 16–24. https://doi.org/10.48009/4_iis_2023_102.