УДК 004-049.5:004.774]351.746.1(477)
DOI https://doi.org/10.32782/2312-1815/2024-18-30

Михайло Савлюк
ORCID: 0009-0001-9870-8343

ВАЖЛИВІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІАЛЬНИХ МЕРЕЖАХ ДЛЯ ЗАГАЛЬНОНАЦІОНАЛЬНОЇ БЕЗПЕКИ: БЕЗПЕКОВИЙ ВИМІР ЕКРАЇНИ

Актуальність проблеми. У XXI столітті разом зі стрімким зростанням новітніх технологій і поширенням Інтернету виникли нові можливості для комунікацій. Особливо це питання стало актуальним і популярним для людей, які спілкуються на відстані. Зі зростанням популярності спілкування в Мережі почали виникати різноманітні платформи для такого спілкування. Спочатку це були форуми, чати й інші платформи. Але у 2004 році, коли американській студент Марк Цукеберг створив першу всесвітньо популярну соціальну мережу Facebook, усе докорінно змінилося. Із зростанням популярності вказаної соціальної мережі та все більше розвивалася, і для неї інженерами розроблявся все більший функціонал. На базі Facebook стало можливим створювати окремі тематичні сторінки, групи та розшукувати знайомих людей. За певний час ця соціальна мережа стала популярною серед дуже значної кількості людей у світі. Завдяки її широкому функціоналу нею зацікавились політики, шахраї та спецслужби різних урядів світу. Із розширенням функціоналу соцмережі та зростанням її популярності у світі, її можливості взялися вивчати різні науковці та світові спецслужби. Через можливість «достукатися» до кожного користувача в цій соціальній мережі та таргетувати (спроєктувати) на нього найрізноманітніші меседжі-послання, Facebook (а згодом й інші соціальні мережі) став небезпечним знаряддям маніпуляції і впливу в руках умілих спеціалістів зі спецслужб різних країн. Відому компанію Cambridge Analitica звинуватили в тому, що вона могла втручалася у вибори в усьому світі, викрадаючи в соціальних мережах персональні дані потенційних виборців і маніпулюючи їх думкою за допомогою спеціальних інформаційних технологій. Значна частина даних була отримана Cambridge Analitica саме від компанії Facebook. Інформаційний скандал щодо можливого незаконного використання персональних даних компанією Cambridge Analitica виник у 2017 році після несподіваної для багатьох експертів перемоги в президентських перегонах у США Дональда Трампа. При цьому медійними розслідувачами був виявлений зв'язок між Cambridge Analytica, Facebook і членами команди новообраного президента США Дональда Трампа. У березні 2018 року світові мас-медіа опублікували результати ще декількох розслідувань, які висвітлюють природу досліджень Cambridge Analitica та передачу компанії приватних даних численних користувачів Facebook. Наразі функціонал указаної соцмережі й багатьох інших популярних соціальних мереж став набагато ширшим і потужнішим, аніж це було сім років тому, а тому соціальні мережі почали нести ще більшу небезпеку. І це стосується не тільки окремих користувачів як індивідуальних одиниць. Комплексний підхід ворожих спецслужб тепер несе загрозу й національній безпеці окремих держав загалом. Саме через популярні соціальні мережі, такі як Facebook, Instagram, YouTube, TikTok, Telegram та інші, спецслужби маніпулюють свідомістю людей, організовуючи та проводячи саме через соціальні мережі так звані ІПСО (інформаційні психологічні спеціальні операції). Соцмережі є дуже важливим інструментом у руках спецслужб для проведення ІПСО. Це пов'язано з поширеністю та популярністю соціальних мереж, а також відносною дешевизною таких платформ порівняно з іншими каналами поширення інформації.

Мета – проаналізувати розробки українських і світових науковців у сфері дослідження масових комунікацій і соціальних мереж, а також через реальні приклади, вивчити методи й алгоритми застосування інформаційних атак ворога, у яких він через свої ІПСО загрожує національній безпеці, зокрема України.

Методи. У межах цієї наукової статті використовувалися такі методи дослідження, як аналіз, синтез, спостереження, емпіричні знання та порівняння.

Результати дослідження. Кінцевою метаю цього наукового дослідження має стати підготовка посібника методичних рекомендацій для пересічного споживача інформаційних послуг (користувача соціальних мереж) і, можливо, працівників спецслужб, де буде розроблено чіткий алгоритм (курс з

інформаційної безпеки та інформаційної гігієни), за допомогою якого можна буде навчитись, як не стати черговою жертвою ворожих ІПСО.

Ключові слова: *ІПСО, інформаційна безпека, кібербезпека, соціальні мережі пропаганда, інформаційні операції, війна, таргетинг, інформаційні атаки, національна безпека.*

Вступ. В епоху стрімкого розвитку інформаційних технологій і глобалізації комунікаційних процесів питання інформаційної безпеки набуває першочергового значення для національної безпеки держав. Особливо гостро ця проблема постає в контексті соціальних мереж, які стали не лише платформою для спілкування, але й потужним інструментом впливу на суспільну думку й національну безпеку. Для України, яка перебуває у стані гібридної війни, забезпечення інформаційної безпеки в соціальних мережах є критично важливим завданням [11].

Актуальність дослідження зумовлена тим, що соціальні мережі стали ареною інформаційного протистояння, де відбуваються спроби маніпулювання громадською думкою, поширення дезінформації та проведення інформаційно-психологічних операцій. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни становлять суттєву небезпеку для національної безпеки України [4, 15].

На жаль, на сучасному етапі українська наука не приділяє особливої уваги соціальним мережам (а саме їхній потенційній загрозі національній безпеці держави), на відміну від західних науковців і західних урядів. У західній науковій думці вже є цілий ряд наукових публікацій про потенційну загрозу національній безпеці через окремі соціальні мережі [24].

Серед науковців, які ретельно досліджують цю тематику, варто вказати американського науковця Лоуренса Траутмана, болгарських дослідниць Габріелу Бєлову та Гергану Геогієву. Серед вітчизняних науковців публікації на таку тематику вже присутні у В. Наместніка, В. Люля й інших.

Матеріалами та методами дослідження виступають публікації вітчизняних та іноземних науковців, які були проаналізовані шляхом теоретико-методологічного дослідження, а також шляхом емпіричних знань, адже автор публікації вже близько 15 років працює у сфері журналістики й тісно взаємодіє із соціальними мережами.

Мета цього дослідження полягає у всебічному аналізі ролі інформаційної безпеки в соціальних мережах у контексті загальнонаціональної безпеки України. Для досягнення цієї мети поставлено такі завдання:

– Визначити теоретичні основи інформаційної безпеки в системі національної безпеки.

– Проаналізувати специфіку інформаційних загроз у соціальних мережах в українському контексті.

– Розглянути роль соціальних мереж у гібридній війні проти України.

– Дослідити законодавчі й організаційні аспекти забезпечення інформаційної безпеки в Україні.

– Запропонувати стратегії протидії інформаційним загрозам у соціальних мережах.

Теоретичні основи інформаційної безпеки в контексті національної безпеки

Інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається нанесення шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання й порушення цілісності, конфіденційності та доступності інформації [20].

Національна безпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз [21].

Інформаційна безпека відіграє ключову роль у забезпеченні національної безпеки держави. Інформаційна боротьба є важливим фактором національної безпеки України. В умовах

інформаційного суспільства захист інформаційного простору стає таким же важливим, як і захист фізичних кордонів держави [13].

Інформаційна могутність стала критичним компонентом національної могутності поряд з економічною, дипломатичною та військовою силою. Здатність держави захищати свій інформаційний простір та ефективно діяти в кіберпросторі є ключовим фактором її національної безпеки у 21-му столітті [26].

Особливості інформаційної безпеки в епоху соціальних мереж

Соціальні мережі стали середовищем проведення інформаційно-психологічних операцій противника. Вони є потужним інструментом впливу на суспільну думку й національну безпеку через їх масовість, швидкість поширення інформації та можливість таргетування аудиторії [17].

Соціальні мережі створюють унікальні виклики для національної безпеки через можливість швидкого поширення чутливої інформації, організації масових заходів і координації дій, потенційно небезпечних для держави [23].

Феномен фейкових новин став суттєвою загрозою національній безпеці. Соціальні мережі стали ідеальним середовищем для поширення дезінформації, яка може підривати стабільність держави та довіру громадян до інституцій влади [24].

Інформаційні загрози в соціальних мережах: український контекст

У контексті України інформаційні загрози в соціальних мережах набувають особливої гостроти. Дезінформація є ключовою складовою інформаційно-психологічних операцій (ІПСО) в умовах російсько-української війни. Можна виділити такі типи інформаційних загроз:

– Поширення неправдивої або викривленої інформації.
– Маніпулювання суспільною думкою.
– Підрив довіри до державних інституцій.
– Провокування панічних настроїв.
– Розпалювання міжнаціональної ворожнечі [15].

Окремо слід виділити наративи формування зневіри як особливий вид ІПСО, спрямований на підрив морального духу населення [22].

Соціальні мережі стали ідеальною платформою для проведення інформаційних атак через ряд факторів:

– Масовість охоплення аудиторії.
– Швидкість поширення інформації.
– Можливість таргетування контенту.
– Складність верифікації джерел інформації.
– Емоційний характер сприйняття контенту користувачами.
– Соціальні мережі дають змогу противнику проводити ІПСО з високою ефективністю та низькими витратами, що робить їх особливо привабливими для інформаційних агресорів [17].

В умовах гібридної війни проти Росії Україна стикається з унікальними викликами в інформаційній сфері. Можна виділити такі специфічні загрози для України:

– Підрив національної ідентичності та єдності.
– Дискредитація української армії та керівництва держави.
– Просування наративів «братніх народів» і «громадянської війни».
– Маніпулювання історичною пам’яттю.
– Провокування внутрішніх конфліктів на релігійному та мовному ґрунті [18].

Особливістю інформаційних загроз для України є їх комплексний характер, який поєднує елементи пропаганди, дезінформації та психологічного тиску [12].

Гібридна війна й інформаційна безпека України

Гібридна війна визначається як ключовий інструмент російської геостратегії реваншу. Вона характеризується як комплекс різноманітних впливів на противника: інформаційних,

психологічних, економічних і військових, які застосовуються комплексно для досягнення політичних цілей [10].

Гібридна війна розглядається як ключова загроза національному суверенітету України. Інформаційна складова є центральним елементом гібридної війни, який дає змогу агресору досягати своїх цілей без широкомасштабного застосування військової сили [19].

Соціальні мережі відіграють критичну роль у веденні гібридної війни проти України. Можна виділити такі аспекти використання соціальних мереж у гібридній війні:

– Формування альтернативної реальності.
– Поляризація суспільства.
– Мобілізація прихильників агресора.
– Дезорієнтація та деморалізація населення.
– Збір розвідувальної інформації [4].

З початком повномасштабного вторгнення Росії проти України, інформаційно-психологічні операції в соціальних мережах значно інтенсифікувалися й набули нових форм [14].

Інформаційно-психологічні операції (ІПСО) в соціальних мережах стали ключовим елементом гібридної війни проти України. Можна виділити такі організаційні аспекти проведення ІПСО:

– Створення мереж ботів і фейкових акаунтів.
– Використання лідерів думок та псевдоекспертів.
– Координація дій через закриті групи та канали.
– Застосування технологій глибинних фейків.
– Використання алгоритмів соціальних мереж для посилення ефекту [7].

ІПСО в соціальних мережах спрямовані не лише на населення України, але й на міжнародну спільноту з метою формування вигідної для агресора картини подій [2].

Законодавчі й організаційні аспекти забезпечення інформаційної безпеки в Україні

Забезпечення інформаційної безпеки в Україні регулюється низкою законодавчих актів. Ключовими документами у цій сфері є:

– Закон України «Про національну безпеку України».
– Закон України «Про інформацію».
– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
– Доктрина інформаційної безпеки України [8].

Інформаційна безпека розглядається як об’єкт посягання злочинів проти основ національної безпеки України, що відображено в Кримінальному кодексі України [3].

До ключових інституцій, відповідальних за забезпечення інформаційної безпеки в Україні, належать:

– Рада національної безпеки і оборони України.
– Служба безпеки України.
– Міністерство інформаційної політики України.
– Національна рада України з питань телебачення і радіомовлення.
– Державна служба спеціального зв’язку та захисту інформації України.

Координація дій цих інституцій є необхідною для ефективного протистояння інформаційним загрозам [6].

Після повномасштабного вторгнення Росії в Україну у 2022 році відбулася суттєва трансформація законодавства у сфері інформаційної безпеки. Ще до повномасштабного вторгнення наголошувалося на необхідності адаптації державної інформаційної політики до умов гібридної війни [16].

Ключові зміни передбачають:

– Посилення відповідальності за поширення дезінформації.

– Розширення повноважень органів державної влади щодо блокування інформаційних ресурсів, які становлять загрозу національній безпеці.

– Впровадження механізмів швидкого реагування на інформаційні атаки.

– Посилення захисту критичної інформаційної інфраструктури.

Стратегії протидії інформаційним загрозам у соціальних мережах

Важливість використання технологічних рішень для управління інформаційною безпекою є критичною. У контексті протидії інформаційним загрозам у соціальних мережах можна виділити такі технологічні стратегії:

– Використання систем штучного інтелекту для виявлення та блокування фейкових акаунтів і ботів.

– Впровадження алгоритмів для автоматичного виявлення дезінформації.

– Розробка інструментів для верифікації контенту та джерел інформації.

– Створення систем моніторингу та аналізу інформаційного простору в режимі реального часу.

– Впровадження технологій блокчейн для забезпечення цілісності та достовірності інформації [25].

Підвищення інформаційної грамотності населення є ключовим фактором протидії інформаційним загрозам. Освітні та просвітницькі ініціативи можуть передбачати:

– Впровадження курсів з медіаграмотності в шкільну й університетську програми.

– Проведення інформаційних кампаній щодо розпізнавання фейкових новин і маніпуляцій.

– Організація тренінгів та семінарів з інформаційної безпеки для різних груп населення.

– Створення освітніх платформ і ресурсів з питань інформаційної безпеки.

– Підтримка громадських ініціатив, спрямованих на підвищення інформаційної культури суспільства [5].

Міжнародне співробітництво у протидії інформаційним загрозам є особливо важливим в умовах гібридної війни. Ключові напрямки міжнародної співпраці такі:

– Обмін досвідом і кращими практиками з протидії інформаційним загрозам.

– Координація зусиль з виявлення та блокування джерел дезінформації.

– Спільна розробка міжнародних стандартів і протоколів інформаційної безпеки.

– Створення міжнародних платформ для швидкого обміну інформацією про кібератаки й інформаційні загрози.

– Проведення спільних навчань і тренувань з кібербезпеки та інформаційної оборони [9].

– Міжнародне співробітництво особливо важливе для України в контексті протистояння російській інформаційній агресії, оскільки дає змогу залучити додаткові ресурси й експертизу для захисту національного інформаційного простору [1].

Проведене дослідження дозволяє зробити такі висновки щодо важливості інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки України:

Інформаційна безпека в соціальних мережах стала критичним компонентом національної безпеки України, особливо в умовах гібридної війни. Соціальні мережі перетворилися на ключовий інструмент інформаційного впливу, що використовується для підриву національної безпеки та стабільності держави [4, 17].

Специфіка інформаційних загроз в українському контексті характеризується комплексним характером, поєднуючи елементи дезінформації, маніпуляції суспільною думкою та психологічного тиску. Ці загрози спрямовані на підрив національної ідентичності, дискредитацію державних інституцій і провокування внутрішніх конфліктів [15, 18].

Гібридна війна, яку веде Росія проти України, значно посилила роль інформаційно-психологічних операцій у соціальних мережах. Ці операції стали невід'ємною частиною стратегії агресора, спрямованої на дестабілізацію українського суспільства та послаблення обороноздатності держави [10, 19].

Законодавча база й інституційні механізми забезпечення інформаційної безпеки в Україні зазнали суттєвої трансформації після повномасштабного вторгнення Росії. Ці зміни спрямовані

на посилення захисту інформаційного простору та протидію інформаційним загрозам, але потребують подальшого вдосконалення й адаптації до швидко змінюваних умов інформаційного протистояння [8, 16].

Ефективна протидія інформаційним загрозам у соціальних мережах вимагає комплексного підходу, що передбачає технологічні рішення, освітні ініціативи та міжнародне співробітництво. Особливу увагу слід приділити підвищенню інформаційної грамотності населення та розвитку критичного мислення як ключових факторів стійкості суспільства до інформаційних маніпуляцій [5, 25].

Рекомендації щодо посилення інформаційної безпеки України в контексті соціальних мереж:

– Розробка та впровадження національної стратегії інформаційної безпеки в соціальних мережах, яка б враховувала специфіку сучасних загроз і технологічних можливостей.

– Посилення координації між різними державними органами, відповідальними за інформаційну безпеку, для забезпечення швидкого реагування на інформаційні атаки.

– Інвестування в розробку вітчизняних технологічних рішень для моніторингу, аналізу та протидії інформаційним загрозам у соціальних мережах.

– Розширення програм з медіаграмотності та критичного мислення на всіх рівнях освіти, а також проведення масштабних інформаційних кампаній для підвищення обізнаності населення щодо інформаційних загроз.

– Активізація міжнародного співробітництва у сфері інформаційної безпеки, включаючи обмін досвідом, спільні навчання та розробку міжнародних стандартів протидії інформаційним загрозам [6, 9, 13, 25].

Результати дослідження вказують, що соціальні мережі несуть досить значну потенційну загрозу для національної безпеки нашої держави, адже ворог досконало освоїв методи інформаційно психологічного впливу на їхніх користувачів. І якщо не робити навчально-методичних матеріалів щодо інформаційної безпеки й інформаційної гігієни користувачів в мережі Інтернет, то такі загрози будуть щоразу тільки зростати та посилюватися.

Висновки. Перспективами подальших досліджень у цій галузі є вивчення впливу нових технологій, таких як штучний інтелект і квантові обчислення, на інформаційну безпеку в соціальних мережах, а також розробка методологій оцінки ефективності заходів з протидії інформаційним загрозам у контексті національної безпеки.

Забезпечення інформаційної безпеки в соціальних мережах залишається критично важливим завданням для України, вирішення якого вимагає постійної уваги, інновацій та адаптації до нових викликів інформаційної епохи [20, 26].

Література:

1. Авер'янова Н. М. Гібридна війна: російсько-українське протистояння. *Молодий вчений*. 2017. № 3. С. 30–34.

2. Алещенко В. Феноменологія гібридної війни та її особливості у виконанні російської федерації: інформаційно-психологічний аспект. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2016. № 1. С. 6–11.

3. Аніщук В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2023. № 2.77. С. 139–143.

4. Арабаджиєв Д. Ю., Сергієнко Т. І. Маніпулювання свідомістю суспільства в умовах інформаційної та гібридної війни в Україні. *Гілея: науковий вісник*. 2019. № 146 (3). С. 12–15.

5. Бєльська Т. В., Крюков О. І. Інформаційні війни та інформаційна безпека: загрози та виклики для демократії. 2019.

6. Богданович В. Ю., Ворович Б. О., Марко Є. І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 3. С. 44–48.

7. Благодарний А. М., Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 48–54.

8. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. 2017.

9. Волос Б. О. Інформаційна безпека України в умовах гібридної війни: внутрішньополітичний аспект. *Традиції та інновації*. 2017. № 298.

10. Горбулін В. П. Гібридна війна як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети*. 2014. № 4.33. С. 5–12.

11. Гулай В. В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової гібрідної війни Російської Федерації проти України. *Військово-науковий вісник.* 2016. № 25. С. 233–244.

12. Даценко А. Протидія дезінформаційним кампаніям в умовах гібридної війни. *Україна в умовах трансформації міжнародної системи*. 2019. № 141.

13. Жарков Я. М., Онищук М. І. Інформаційна боротьба як фактор національної безпеки України. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2015. № 50. С. 87–92.

14. Іванова В. Трансформація інформаційно-психологічних операцій Російської Федерації з початком повномасштабної агресії проти України. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : матеріали IV міжнар. наук.-практ. конф. 2023.

15. Кутуза Н. В., Тельпіс Д. М. Дезінформація як складник ІПСО в мегадискурсі: маніпулятивний аспект (на прикладі російсько-української війни періоду повномасштабного вторгнення). *Записки з українського мовознавства*. 2023. № 30. С. 282–292.

16. Лісовська О. Л. Пріоритети державної інформаційної політики в Україні в умовах гібридної війни. *Актуальні проблеми управління інформаційною безпекою держави*. 2019. № 83.

17. Наместнік В. Соціальні мережі як середовище проведення інформаційно-психологічних операцій противника. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : матеріали IV міжнар. наук.-практ. конф. 2023.

18. Нофенко А. Гібридна війна Росії проти України: інформаційний наступ та механізми протидії. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2019. № 2 (6). С. 68–77.

19. Радченко О. В., Чмир Я. І. Гібридна війна як ключова загроза національному суверенітету України. *Таврійський науковий вісник. Серія : Публічне управління та адміністрування*. 2021. № 3. С. 100–108.

20. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2 (5). С. 162–169.

21. Чичеба Д. О., Жовтенко Т. Г., Крет Р. М. Інформаційна безпека як складова національної безпеки.

22. Шульська Н. М., Зінчук Р. С., Кевлюк І. В. Наративи формування зневіри як вияв ворожої інформаційно-психологічної операції: на матеріалі мови ЗМІ. *Вчені записки*. 2023. № 22023152.

23. Abdulhamid S.M. et al. Privacy and national security issues in social networks: the challenges. arXiv preprint arXiv:1402.3301. 2014.

24. Belova G., Georgieva G. Fake news as a threat to national security. *International conference knowledge-based organization*. 2018. Vol. 24, № 1.

25. Choobineh J. et al. Management of information security: Challenges and research directions. *Communications of the Association for Information Systems.* 2007. Vol. 20, № 1. P. 57.

26. Kramer F. D., Starr S.H., Wentz L. K. (Eds.). Cyberpower and national security. Potomac Books, Inc., 2009.

References:

1. Averianova, N. M. (2017). Hibrydna viina: rosiisko-ukrainske protystoiannia [Hybrid war: Russian-Ukrainian confrontation]. *Molodyi vchenyi* – Young Scientist, 3, 30–34 [in Ukrainian].

2. Aleshchenko, V. (2016). Fenomenolohiia hibrydnoi viiny ta yii osoblyvosti u vykonanni rosiiskoi federatsii: informatsiino-psykholohichnyi aspekt [Phenomenology of hybrid warfare and its features in the performance of the Russian Federation: information-psychological aspect]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky* – Bulletin of Taras Shevchenko National University of Kyiv. Military Special Sciences, 1, 6–11 [in Ukrainian].

3. Anishchuk, V. (2023). Informatsiina bezpeka yak obiekt posiahannia zlochyniv proty osnov natsionalnoi bezpeky Ukrainy [Information security as an object of encroachment of crimes against the foundations of national security of Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Scientific Bulletin of Uzhhorod National University*. Series: Law, 2.77, 139–143 [in Ukrainian].

4. Arabadzhyiev, D.Yu., & Serhiienko, T.I. (2019). Manipuliuvannia svidomistiu suspilstva v umovakh informatsiinoi ta hibrydnoi viiny v Ukraini [Manipulation of public consciousness in the conditions of information and hybrid war in Ukraine]. *Hileia: naukovyi visnyk – Gilea: Scientific Bulletin*, 146(3), 12–15 [in Ukrainian].

5. Bielska, T.V., & Kriukov, O.I. (2019). Informatsiini viiny ta informatsiina bezpeka: zahrozy ta vyklyky dlia demokratii [Information wars and information security: threats and challenges for democracy] [in Ukrainian].

6. Bohdanovych, V.Yu., Vorovych, B.O., & Marko, Ye.I. (2018). Informatsiina bezpeka yak osnova voiennoi bezpeky derzhavy ta suspilstva [Information security as the basis of military security of the state and society]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho* – Collection of Scientific Papers of the Center for Military-Strategic Studies of the National Defense University of Ukraine named after Ivan Cherniakhovskyi, 3, 44–48 [in Ukrainian].

7. Blahodarnyi, A.M., & Shtelmakh, O.V. (2015). Orhanizatsiini aspekty protydii informatsiinii ahresii yak skladovii hibrydnoi viiny [Organizational aspects of counteracting information aggression as a component of hybrid warfare]. Informatsiina bezpeka liudyny, suspilstva, derzhavy – Information Security of the Individual, Society, State, 3, 48–54 [in Ukrainian].

8. Valiushko, I.O. (2017). Informatsiina bezpeka Ukrainy: transformatsiia zakonodavstva pislia rosiiskoho vtorhnennia [Information security of Ukraine: transformation of legislation after the Russian invasion] [in Ukrainian].

9. Volos, B.O. (2017). Informatsiina bezpeka Ukrainy v umovakh hibrydnoi viiny: vnutrishnopolitychnyi aspekt [Information security of Ukraine in the conditions of hybrid war: internal political aspect]. Tradytsii ta innovatsii – Traditions and Innovations, 298 [in Ukrainian].

10. Horbulin, V.P. (2014). Hibrydna viina yak kliuchovyi instrument rosiiskoi heostratehii revanshu [Hybrid war as a key tool of Russian geostrategy of revenge]. Stratehichni priorytety – Strategic Priorities, 4 (33), 5–12 [in Ukrainian].

11. Hulai, V.V. (2016). Zahrozy informatsiino-psykholohichnii bezpetsi osoby v realiiakh informatsiino-psykholohichnoi viiny yak skladovoi hibrydnoi viiny Rosiiskoi Federatsii proty Ukrainy [Threats to information and psychological security of a person in the realities of information and psychological war as a component of the hybrid war of the Russian Federation against Ukraine]. *Viiskovo-naukovyi visnyk* – Military-Scientific Bulletin, 25, 233–244 [in Ukrainian].

12. Datsenko, A. (2019). Protydiia dezinformatsiinym kampaniiam v umovakh hibrydnoi viiny [Counteraction to disinformation campaigns in the conditions of hybrid warfare]. Ukraina v umovakh transformatsii mizhnarodnoi systemy – Ukraine in the Conditions of Transformation of the International System, 141 [in Ukrainian].

13. Zharkov, Ya.M., & Onyshchuk, M.I. (2015). Informatsiina borotba yak faktor natsionalnoi bezpeky Ukrainy [Information struggle as a factor of national security of Ukraine]. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka – Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv, 50, 87–92 [in Ukrainian].

14. Ivanova, V. (2023). Transformatsiia informatsiino-psykholohichnykh operatsii Rosiiskoi Federatsii z pochatkom povnomasshtabnoi ahresii proty Ukrainy [Transformation of information and psychological operations of the Russian Federation with the beginning of full-scale aggression against Ukraine]. Proceedings from Strategic Communications in the Field of National Security and Defense: Problems, Experience, Prospects: IV International Scientific and Practical Conference [in Ukrainian].

15. Kutuza, N.V., & Telpis, D.M. (2023). Dezinformatsiia yak skladnyk IPSO v mehadyskursi: manipuliatyvnyi aspekt (na prykladi rosiisko-ukrainskoi viiny periodu povnomasshtabnoho vtorhnennia) [Disinformation as a component of IPSO in megadiscourse: manipulative aspect (on the example of the Russian-Ukrainian war during the full-scale invasion)]. *Zapysky z ukrainskoho movoznavstva* – Notes on Ukrainian Linguistics, 30, 282–292 [in Ukrainian].

16. Lisovska, O.L. (2019). Priorytety derzhavnoi informatsiinoi polityky v Ukraini v umovakh hibrydnoi viiny [Priorities of state information policy in Ukraine in the conditions of hybrid warfare]. Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy – Actual Problems of State Information Security Management, 83 [in Ukrainian].

17. Namestnik, V. (2023). Sotsialni merezhi yak seredovyshche provedennia informatsiino-psykholohichnykh operatsii protyvnyka [Social networks as an environment for conducting information and psychological operations of the enemy]. Proceedings from Strategic Communications in the Field of National Security and Defense: Problems, Experience, Prospects : IV International Scientific and Practical Conference [in Ukrainian].

18. Nofenko, A. (2019). Hibrydna viina Rosii proty Ukrainy: informatsiinyi nastup ta mekhanizmy protydii [Russia's hybrid war against Ukraine: information offensive and counteraction mechanisms]. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii – International Relations, Public Communications and Regional Studies*, 2(6), 68–77 [in Ukrainian].

19. Radchenko, O.V., & Chmyr, Ya.I. (2021). Hibrydna viina yak kliuchova zahroza natsionalnomu suverenitetu Ukrainy [Hybrid war as a key threat to Ukraine's national sovereignty]. *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia – Taurian Scientific Bulletin. Series: Public Administration*, 3, 100–108 [in Ukrainian].

20. Furashev, V.M. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and information space, cybersecurity and information security: essence, definitions, differences]. *Informatsiia i pravo – Information and Law*, 2 (5), 162–169 [in Ukrainian].

21. Chycheba, D.O., Zhovtenko, T.H., & Kret, R.M. (n.d.). Informatsiina bezpeka yak skladova natsionalnoi bezpeky [Information security as a component of national security] [in Ukrainian].

22. Shulska, N.M., Zinchuk, R.S., & Kevliuk, I.V. (2023). Naratyvy formuvannia zneviry yak vyiav vorozhoi informatsiino-psykholohichnoi operatsii: na materiali movy ZMI [Narratives of forming despair as a manifestation of hostile information and psychological operation: based on the language of the media]. *Vcheni zapysky – Scientific Notes*, 22023152 [in Ukrainian].

23. Abdulhamid, S.M., et al. (2014). Privacy and national security issues in social networks: the challenges. Ar Xiv preprint arXiv:1402.3301 [in English].

24. Belova, G., & Georgieva, G. (2018). Fake news as a threat to national security. *International conference knowledge-based organization,* 24 (1). [in English].

25. Choobineh, J., et al. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, 20 (1), 57 [in English].

26. Kramer, F. D., Starr, S. H., & Wentz, L. K. (Eds.). (2009). Cyberpower and national security. Potomac Books, Inc. [in English].

Mykhailo Savliuk. The importance of information security in social networks for national security: security dimension of Ukraine

Relevance of the problem. In the 21st century, along with the rapid growth of new technologies and the spread of the internet, new opportunities for communication have emerged. This issue has become particularly relevant and popular for people who communicate at a distance. With the growing popularity of communication on the "network," various platforms for such communication began to appear. Initially, these were forums, chats, and other platforms. But in 2004, when American student Mark Zuckerberg created the first globally popular social network Facebook, everything changed fundamentally. With the growing popularity of this social network, it developed further, and engineers developed more and more functionality for it. On the basis of Facebook, it became possible to create separate thematic pages, groups, and search for acquaintances around the world. Over time, this social network became popular among a very significant number of people worldwide. After this, thanks to its wide functionality, politicians, fraudsters, and special services of various world governments became interested in it. With the expansion of the social network's functionality and its growing popularity worldwide, various scientists and world special services began to study its capabilities. Due to the ability to "reach out" to every user on this social network and target (project) a wide variety of message-messages to them, Facebook (and later other social networks) became a dangerous tool of manipulation and influence in the hands of skilled specialists from special services of different countries worldwide. The world-renowned company Cambridge Analytica was accused of interfering in elections worldwide by stealing personal data of potential voters on social networks and manipulating their opinions using special information technologies. A significant portion of the data was obtained by Cambridge Analytica from Facebook. The information scandal regarding the possible illegal use of personal data by

Cambridge Analytica emerged in 2017 after Donald Trump's unexpected victory in the US presidential race for many experts. Media investigators revealed a connection between Cambridge Analytica, Facebook, and members of newly elected US President Donald Trump's team. In March 2018, global mass media published the results of several more investigations that shed light on the nature of Cambridge Analytica's research and the transfer of private data of numerous Facebook users to the company. Currently, the functionality of this social network, and many other popular social networks, has become much broader and more powerful than it was 7 years ago, and therefore social networks have begun to pose an even greater danger. And this applies not only to individual users as individual units. The comprehensive approach of hostile special services now poses a threat to the national security of individual states as a whole. It is through popular social networks such as Facebook, Instagram, YouTube, TikTok, Telegram, and others that special services manipulate people's consciousness worldwide, organizing and conducting so-called IPSOs (information psychological special operations) through social networks. Social networks are a very important tool in the hands of special services for conducting IPSOs. This is due to the prevalence and popularity of social networks, as well as the relative cheapness of such platforms compared to other channels of information dissemination.

Goal. To analyze the developments of Ukrainian and world scientists in the field of mass communications and social networks research, as well as through real examples, to study the methods and algorithms of applying enemy information attacks, in which it threatens national security, particularly Ukraine, through its IPSOs.

Methods. Within the framework of this scientific article, such research methods as analysis, synthesis, observation, empirical knowledge, and comparison were used.

Research results. The final goal of this scientific research should be the preparation of a manual of methodological recommendations for the average consumer of information services (social network user) and possibly special service employees, where a clear algorithm (course on information security and information hygiene) will be developed, with the help of which it will be possible to learn how not to become another victim of hostile IPSOs.

Key words: *information security, social networks, national security, hybrid warfare, information threats, disinformation, media literacy, cybersecurity, Ukraine.*

Інформація про автора:

Михайло Савлюк – ааспірант кафедри політичних інститутів та процесів,
Прикарпатський національний університет імені Василя Стефаника;
Івано-Франківський міський суд.