АНОТАЦІЯ

Савлюк М. І. Загрози інформаційній безпеці в соціальних мережах під час Війни за Незалежність України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії в галузі знань 05 Соціальні та поведінкові науки за спеціальністю 052 Політологія. – Карпатський національний університет імені Василя Стефаника, Міністерство освіти і науки України, м. Івано-Франківськ, 2026.

У дисертації здійснено комплексне політологічне дослідження сучасних загроз інформаційній безпеці України в середовищі соціальних мереж у контексті Війни за Незалежність України. Соціальні мережі розглядаються як середовище стратегічного впливу, у якому інформаційні потоки використовуються для формування громадської думки, мобілізації/демобілізації аудиторій, впливу на політичні процеси та підриву стійкості держави. Актуальність дослідження зумовлена експоненційним зростанням викликів інформаційній безпеці в умовах цифровізації суспільних комунікацій та трансформації інформаційного простору на один із ключових вимірів національної безпеки. У XXI столітті інформація виступає не лише ресурсом управління й розвитку, а й інструментом впливу, здатним визначати суспільні настрої, поведінкові моделі, легітимність політичних інститутів і стійкість держави до зовнішнього тиску. Відтак інформаційна безпека набуває характеру системоутворюючого чинника державності, оскільки безпосередньо пов'язана із захистом суверенітету, демократичних процедур, ціннісних орієнтирів і спроможності держави здійснювати ефективну політику в умовах кризових викликів.

Мета дослідження полягає у всебічному аналізі загроз інформаційній безпеці в соціальних мережах в умовах Війни за Незалежність України та обґрунтуванні механізмів захисту й підвищення стійкості інформаційного простору України на основі українського та міжнародного досвіду. Відповідно до мети визначено такі завдання: розкрити сутність поняття інформаційної

безпеки як політологічної категорії та визначити її структурні компоненти, функції й особливості; узагальнити теоретичні підходи та методи дослідження інформаційної безпеки й обґрунтувати методологічний інструментарій дисертації; проаналізувати нормативно-правову базу у сфері забезпечення інформаційної безпеки України; дослідити соціальні мережі як інструмент стратегічного впливу; охарактеризувати інформаційно-психологічні операції в соціальних мережах; проаналізувати кіберзагрози та технічні інструменти ведення гібридної війни; здійснити аналіз ключових кейсів інформаційного впливу на Україну у 2014–2025 рр.; узагальнити вітчизняний і світовий досвід протидії інформаційним загрозам; розробити практичні рекомендації щодо удосконалення механізмів захисту та підвищення стійкості інформаційного простору України.

Об'єктом дослідження є особливості формування та функціонування інформаційної безпеки України в умовах зовнішніх загроз і впливів. Предметом дослідження є загрози інформаційній безпеці України в соціальних мережах в умовах гібридної війни, механізми та закономірності їх виявлення й нейтралізації, з урахуванням вітчизняного та міжнародного досвіду.

Методологічну основу становить поєднання системного та компаративного аналізу, документального аналізу нормативно-правової бази, контент- та івент-аналізу, кейс-стаді, SWOT-аналізу й елементів прогнозування, що забезпечує комплексне вивчення загроз, інструментів впливу та практик протидії. Аналітичний метод застосовано під час опрацювання історіографії, концептуальних підходів і ключових категорій. Метод системного аналізу дав змогу розглядати інформаційну безпеку як складну систему взаємопов'язаних елементів – нормативно-правової бази, інституційної архітектури, механізмів координації, комунікаційних практик, технологічних чинників та зовнішніх впливів. Для оцінювання регуляторних засад і практик державного реагування застосовано метод документального аналізу; для зіставлення підходів України з практиками держав-партнерів – компаративний метод; для глибокого вивчення конкретних проявів інформаційного впливу – метод кейс-стаді; для виявлення

структури, змісту й динаміки інформаційних повідомлень – контент-аналіз; для оцінювання внутрішніх і зовнішніх чинників, що визначають спроможність держави забезпечувати інформаційну безпеку, – SWOT-аналіз. Метод моделювання використано для побудови узагальнених моделей інституційного механізму, а метод прогнозування – для визначення потенційних сценаріїв розвитку інформаційно-безпекової ситуації в Україні.

У першому розділі закладено теоретичний фундамент дослідження та сформовано категорійно-понятійний каркас аналізу. Розкрито сутність інформаційної безпеки, її структурні компоненти, функції та особливості як складника національної безпеки; показано, що інформаційна безпека у політологічному вимірі виходить за межі технічного захисту й включає політичні, соціальні та правові параметри управління інформаційними потоками. Встановлено, що поняття «інформаційна безпека» увійшло до наукового обігу наприкінці 1980-х років і з суто технічної категорії поступово трансформувалося в комплексний науковий конструкт, що охоплює проблеми захисту інформаційних ресурсів, стабільності інформаційного простору, протидії інформаційним загрозам і забезпечення національних інтересів держави. Обґрунтовано, що в сучасному розумінні інформаційна безпека – це стан захищеності основних інтересів особи, суспільства та держави в інформаційній сфері, що охоплює інформаційну та телекомунікаційну інфраструктуру, а також саму інформацію з її характеристиками: повнотою, об'єктивністю, доступністю та конфіденційністю. Проаналізовано багаторівневий характер сучасних загроз, які охоплюють: технологічний вимір (кібератаки, компрометація акаунтів, витоки даних); когнітивно-психологічний вимір (маніпуляції, дезінформація, нав'язування деструктивних наративів); інституційно-політичний вимір (підрив довіри до державних інституцій, вплив на електоральні процеси); соціальний вимір (поляризація, фрагментація суспільства); міжнародний вимір (вплив на міжнародну підтримку України). Здійснено аналіз нормативно-правової бази забезпечення інформаційної та кібербезпеки України, розглянуто її роль як інструменту державного управління

й політичного регулювання інформаційних процесів та окреслено значення законодавчих і стратегічних документів для превентивного виявлення загроз і координації дій суб'єктів безпеки.

Другий розділ присвячено розкриттю логіки гібридної війни в інформаційному вимірі та демонстрації того, як соціальні мережі стають платформним середовищем реалізації впливів. Соціальні мережі розглянуто як інструмент стратегічного впливу: обґрунтовано їхню роль у формуванні суспільної думки, політичних процесів і безпекових ризиків; показано, що мережна архітектура платформ, швидкість поширення контенту, алгоритмічна персоналізація та низький поріг входу для продукування інформаційних повідомлень створюють сприятливі умови для реалізації деструктивних впливів. Проаналізовано інформаційно-психологічні операції (ІПсО) в соціальних мережах як ключовий механізм інформаційної війни: окреслено їхні цілі – підрив легітимності влади, зниження суспільної згуртованості, деморалізація населення, формування вигідних агресору поведінкових моделей, – а також специфіку їхньої результативності завдяки швидкому доступу до великих аудиторій і механізмам мікротаргетингу. Виявлено, що ІПсО спрямовані одночасно на внутрішню аудиторію (деморалізація, поляризація, підрив довіри до влади) та зовнішню (дискредитація України в очах міжнародної спільноти). Розкрито кіберзагрози та технічні інструменти гібридної війни: від зламів акаунтів і фішингових атак до автоматизованих мереж (ботів, «сокпапетів») і технологій маніпуляції контентом (діпфейки, генеративний штучний інтелект). Встановлено, що кіберзагрози функціонують у взаємодоповнювальній єдності з ІПсО, формуючи синергетичний ефект.

У третьому розділі здійснено аналіз ключових кейсів інформаційного впливу на Україну у 2014–2025 рр., що дозволяє простежити еволюцію інструментів і наративів впливу та показати їхній зв'язок із політико-історичними передумовами й загальною ревізіоністською логікою російської політики. Виявлено, що впродовж зазначеного періоду відбулася системна трансформація методів і масштабів інформаційної агресії: від відносно

локалізованих операцій у 2014–2015 рр. до тотального інформаційного наступу в умовах повномасштабного вторгнення 2022–2025 рр. Встановлено стійкі наративні конструкти, що системно відтворюються у різних кейсах і є складниками єдиної стратегії підриву державності та легітимності України. Проаналізовано інституційні механізми протидії: діяльність Центру протидії дезінформації, Центру стратегічних комунікацій та інформаційної безпеки, Державної служби спеціального зв'язку та захисту інформації, Оперативного центру реагування на кіберінциденти та інших суб'єктів. Розглянуто досвід держав-партнерів (Естонія, Фінляндія, Латвія, Литва, Польща, Швеція, США, Великобританія та ін.) у побудові систем протидії дезінформації та кіберзагрозам. Обґрунтовано необхідність комплексного підходу, що включає нормативно-правові, інституційні, комунікаційні та освітні інструменти, а також підвищення стійкості суспільства до дезінформаційних кампаній, розширення міжнародної кооперації та розвиток спроможностей реагування.

Наукова новизна отриманих результатів зумовлена комплексним політологічним осмисленням сучасних загроз інформаційній безпеці в соціальних мережах в умовах гібридної війни та поглибленим аналізом інституційних механізмів протидії таким загрозам. У дисертації соціальні мережі концептуалізовано не лише як канал комунікації, а як середовище стратегічного впливу, де поєднуються ІПсО, маніпулятивні технології, алгоритмічне підсилення контенту, кібератаки та практики координованої неавтентичної поведінки. *Уперше*: комплексно досліджено сучасні загрози інформаційній безпеці України у соціальних мережах як складник гібридної війни; розроблено механізм інституційної взаємодії у сфері протидії загрозам, що враховує багаторівневість суб'єктів (державні органи, сектор безпеки й оборони, медіа, громадянське суспільство, міжнародні партнери, платформи); здійснено типологізацію загроз у соціальних мережах та визначено індикатори їх виявлення; проаналізовано ключові кейси інформаційного впливу (2014–2025 рр.); застосовано SWOT-аналіз і прогнозування до сфери інформаційної безпеки у соціальних мережах. *Удосконалено*: теоретико-методологічні засади

аналізу інформаційної безпеки в умовах диджиталізації; категорійно-понятійний апарат через уточнення співвідношення понять «інформаційна безпека» – «інформаційна агресія» – «ІПсО» – «дезінформація» – «стратегічні комунікації» – «стійкість інформаційного простору»; підхід до аналізу інституційних чинників шляхом виокремлення функційної параметризації завдань (моніторинг, превенція, реагування, кризові комунікації, міжвідомча координація). *Набули подальшого розвитку* положення про роль соціальних мереж у гібридній війні; про значення інституційної спроможності держави у протидії загрозам; про оптимальні моделі поєднання реактивних і проактивних підходів до політики інформаційної безпеки; про механізми міжнародної взаємодії у протидії дезінформації та ІПсО.

Теоретичне значення дослідження визначається тим, що його результати розширюють політологічне розуміння інформаційної безпеки як складника національної безпеки в умовах гібридної війни та цифровізації політичних комунікацій. Сформульовані положення, висновки й узагальнення можуть бути використані у подальших гуманітарних студіях – насамперед у межах політичної науки, а також соціології, культурології, прикладної лінгвістики та соціолінгвістики. Теоретичний внесок роботи полягає також у розкритті ролі інституційних чинників у формуванні стійкості інформаційного простору, виявленні закономірностей розгортання ІПсО та уточненні понятійно-категоріального апарату дослідження загроз інформаційній безпеці в соціальних мережах.

Практичне значення результатів полягає у можливості використання висновків і рекомендацій у діяльності органів публічної влади та сектору безпеки й оборони, у вдосконаленні державної інформаційно-безпекової політики щодо соціальних мереж, посиленні міжвідомчої координації та розвитку технологічних інструментів моніторингу й реагування. Матеріали дисертації можуть бути використані при формуванні й оновленні навчальних курсів за напрямами підготовки «Політологія», «Національна безпека», «Міжнародні відносини», «Інформаційна безпека» та спорідненими

спеціальностями. У ширшій перспективі результати роботи спрямовані на підтримку формування сприятливих умов для розвитку інформаційного суспільства в Україні та зміцнення національної безпеки в умовах тривалої агресії.

Ключові слова: інформаційна безпека, соціальні мережі, гібридна війна, інформаційна агресія, дезінформація, ІПсО, кіберзагрози, стратегічні комунікації, інституційні механізми, стійкість інформаційного простору, національна безпека.

SUMMARY

Savliuk M. I. Threats to Information Security in Social Media during Ukraine's War of Independence. – Qualification scientific work in the rights of a manuscript.

Dissertation submitted for the degree of Doctor of Philosophy in the field of knowledge 05 Social and Behavioral Sciences on specialty 052 Political Science. – Vasyl Stefanyk Carpathian National University, Ministry of Education and Science of Ukraine, Ivano-Frankivsk, 2026.

The dissertation presents a comprehensive political-science study of contemporary threats to Ukraine's information security in the social media environment in the context of the War of Independence of Ukraine. Social media are examined as a domain of strategic influence in which information flows are employed to shape public opinion, mobilise and demobilise audiences, affect political processes, and undermine state resilience. The relevance of the study is driven by the exponential growth of challenges to information security amid the digitalisation of public communications and the transformation of the information space into one of the key dimensions of national security. In the twenty-first century, information serves not merely as a resource for governance and development but as an instrument of influence capable of shaping public sentiment, behavioural patterns, the legitimacy of political institutions, and state resilience to external pressure. Accordingly, information security acquires the character of a system-forming factor of statehood, as it is directly linked to the protection of sovereignty, democratic procedures, value

orientations, and the capacity of the state to implement effective policy under conditions of crisis.

The purpose of the study is to provide an exhaustive analysis of information-security threats in social media under conditions of hybrid warfare and to substantiate protection mechanisms and approaches to enhancing the resilience of Ukraine's information space on the basis of domestic and international experience. In pursuance of this purpose, the following tasks were defined: to clarify the essence of information security as a political-science category and determine its structural components, functions, and specific features; to synthesise theoretical approaches and research methods in information-security studies and substantiate the methodological toolkit of the dissertation; to analyse Ukraine's regulatory and legal framework in the field of information security; to examine social media as an instrument of strategic influence; to characterise information and psychological operations in social media; to analyse cyber threats and the technical instruments of hybrid warfare; to conduct a case-study analysis of key instances of information influence on Ukraine in 2014–2025; to synthesise domestic and international experience in countering information threats; and to develop practical recommendations for improving protection mechanisms and strengthening the resilience of Ukraine's information space.

The object of the study is the specific features of the formation and functioning of Ukraine's information security under conditions of external threats and influences. The subject of the study is the threats to Ukraine's information security in social media under conditions of hybrid warfare, as well as the mechanisms and regularities underlying their identification and neutralisation, taking into account both domestic and international experience.

The methodological framework integrates systems and comparative analysis, documentary analysis of the regulatory and legal base, content analysis and event analysis, case-study methodology, SWOT analysis, and elements of forecasting, thereby enabling a comprehensive examination of threats, instruments of influence, and countermeasure practices. The analytical method was applied in processing the historiography, conceptual approaches, and key categories of the field. Systems

analysis enabled information security to be examined as a complex system of interrelated elements – the regulatory and legal base, institutional architecture, coordination mechanisms, communication practices, technological factors, and external influences. Documentary analysis was used to assess regulatory foundations and state response practices; comparative analysis to juxtapose Ukraine's approaches with those of partner states; case-study methodology for in-depth examination of specific manifestations of information influence; content analysis to identify the structure, content, and dynamics of information messages; and SWOT analysis to evaluate internal and external factors determining state capacity to ensure information security. Modelling was employed to construct generalised models of the institutional mechanism, while forecasting was used to identify potential scenarios for the development of the information-security situation in Ukraine.

Chapter 1 establishes the theoretical foundations of the study and develops the conceptual and categorical framework for analysis. It clarifies the essence of information security, its structural components, functions, and specific features as a component of national security, demonstrating that in political-science terms information security extends beyond technical protection and encompasses political, social, and legal parameters of governing information flows. It is established that the concept of "information security" entered scholarly discourse in the late 1980s and gradually evolved from a purely technical category into a complex scientific construct encompassing the protection of information resources, the stability of the information space, the countering of information threats, and the safeguarding of state interests. It is substantiated that in its contemporary understanding information security constitutes a state of protection of the fundamental interests of the individual, society, and the state in the information sphere, covering information and telecommunication infrastructure as well as information itself in terms of its completeness, objectivity, accessibility, and confidentiality. The chapter analyses the multi-level character of contemporary threats, spanning the technological dimension (cyberattacks, account compromise, data leaks); the cognitive-psychological dimension (manipulation, disinformation, the imposition of destructive narratives);

the institutional-political dimension (undermining trust in state institutions, influencing electoral processes); the social dimension (polarisation, fragmentation of society); and the international dimension (influencing international support for Ukraine). Ukraine's regulatory and legal framework for information and cyber security is analysed, its role as an instrument of public administration and political regulation of information processes is examined, and the significance of legislative and strategic documents for the preventive identification of threats and the coordination of security actors is outlined.

Chapter 2 elucidates the logic of hybrid warfare in the informational dimension and demonstrates how social media become platform-based environments for the operationalisation of influence. Social media are examined as instruments of strategic influence: their role in shaping public opinion, political processes, and security risks is substantiated, and it is shown that the network architecture of platforms, the speed of content dissemination, algorithmic personalisation, and the low entry threshold for producing information messages create favourable conditions for the realisation of destructive influences. Information and psychological operations (IPsO) in social media are analysed as a key mechanism of information warfare: their objectives are identified, undermining the legitimacy of public authority, weakening social cohesion, demoralising the population, and fostering behavioural patterns advantageous to the aggressor and their effectiveness is explained through rapid access to mass audiences and microtargeting mechanisms. It is found that IPsO are directed simultaneously at domestic audiences (demoralisation, polarisation, undermining trust in government) and external ones (discrediting Ukraine in the eyes of the international community). Cyber threats and the technical instruments of hybrid warfare are explicated, from account compromise and phishing attacks to automated networks (bots and sockpuppets) and content-manipulation technologies (deepfakes, generative artificial intelligence), and it is established that cyber threats operate in complementary unity with IPsO, producing a synergistic effect.

Chapter 3 analyses key cases of information influence on Ukraine in 2014–2025, tracing the evolution of instruments and narratives of influence and

demonstrating their linkage to political-historical preconditions and the broader revisionist logic of Russian policy. It is found that over the period under review a systemic transformation of the methods and scale of information aggression took place: from relatively localised operations in 2014–2015 to a total information offensive under conditions of full-scale invasion in 2022–2025. Persistent narrative constructs are identified that are systematically reproduced across different cases and constitute components of a unified strategy aimed at undermining Ukrainian statehood and legitimacy. The institutional mechanisms of counteraction are analysed, including the activities of the Centre for Countering Disinformation, the Centre for Strategic Communications and Information Security, the State Service of Special Communications and Information Protection, the Operational Centre for Responding to Cyber Incidents, and other actors. The experience of partner states (Estonia, Finland, Latvia, Lithuania, Poland, Sweden, the United States, the United Kingdom, and others) in building systems to counter disinformation and cyber threats is examined. The need for a comprehensive approach is substantiated, encompassing regulatory, institutional, communication, and educational instruments, as well as strengthening societal resilience to disinformation campaigns, expanding international cooperation, and developing response capacities.

The scholarly novelty of the study lies in the comprehensive political-science examination of contemporary information-security threats in social media under conditions of hybrid warfare and the in-depth analysis of institutional mechanisms for countering such threats. In the dissertation, social media are conceptualised not merely as a communication channel but as a domain of strategic influence in which IPsO, manipulative technologies, algorithmic content amplification, cyberattacks, and coordinated inauthentic behaviour converge. For the first time: the contemporary threats to Ukraine's information security on social media as a component of hybrid warfare have been comprehensively examined; a mechanism for institutional interaction in the field of threat countermeasures has been developed, incorporating the multi-level structure of actors (state bodies, the security and defence sector, media, civil society, international partners, and platforms); a typology of threats on

social media has been constructed and indicators for their identification have been defined; key cases of information influence operations (2014–2025) have been analysed; SWOT analysis and forecasting methods have been applied to the domain of information security on social media.

Further developed are: the theoretical and methodological foundations of information-security analysis under conditions of digitalisation; the conceptual and categorical apparatus through the clarification of the relationships among "information security", "information aggression", "IPsO", "disinformation", "strategic communications", and "information-space resilience"; and the approach to analysing the institutional factors of information-security policy through the identification of functional task parameters (monitoring, prevention, response, crisis communications, inter-agency coordination). The following propositions have been further developed: the role of social media in hybrid warfare as an instrument of strategic influence; the significance of state institutional capacity in countering threats in social media; optimal models for combining reactive and proactive approaches to information-security policy in wartime; and mechanisms of international cooperation in countering disinformation and IPsO.

The theoretical significance of the study lies in the fact that its results broaden the political-science understanding of information security as a component of national security under conditions of hybrid warfare and the digitalisation of political communications. The formulated propositions, conclusions, and generalisations may be employed in further humanities research – primarily within political science and also within sociology, cultural studies, applied linguistics, and sociolinguistics. The theoretical contribution of the work also consists in elucidating the role of institutional factors in building the resilience of the information space, identifying regularities in the deployment of IPsO, and refining the conceptual and categorical apparatus for studying information-security threats in social media.

The practical significance of the results consists in the possibility of employing the findings and recommendations in the activities of public authorities and the security and defence sector, in improving state information-security policy with

respect to social media, in strengthening inter-agency coordination, and in developing technological tools for monitoring and response. The materials of the dissertation may be used in developing and updating curricula in the fields of Political Science, National Security, International Relations, Information Security, and related specialisations. In a broader perspective, the results of the work are aimed at supporting the creation of favourable conditions for the development of the information society in Ukraine and the strengthening of national security under conditions of protracted aggression.

Keywords: information security; social media; hybrid warfare; information aggression; disinformation; information and psychological operations; cyber threats; strategic communications; institutional mechanisms; information-space resilience; national security.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових виданнях України категорії Б:

1. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки. *Вісник Прикарпатського університету. Серія: Політологія*. 2023. Випуск 15. 2023. С.60-68

DOI: https://doi.org/10.32782/2312-1815/2024-1-8

URL: https://journals.pnu.if.ua/index.php/politology/article/view/54

2. Савлюк М. Гібридна війна в Україні: сучасні підходи. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С.187-197.

DOI: https://doi.org/10.32782/2312-1815/2024-17-23

URL: https://journals.pnu.if.ua/index.php/politology/article/view/130

3. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Випуск 18. С.300-309.

DOI: https://doi.org/10.32782/2312-1815/2024-18-30

URL: https://journals.pnu.if.ua/index.php/politology/article/view/167

4. Пролорензо А. Савлюк М. Кіберзахист як складник інформаційної безпеки держави в умовах гібридної війни. *Національні інтереси України*. 2025. №6 (11). С.198-213

DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-198-213

URL: https://perspectives.pp.ua/index.php/niu/article/view/25245/25222

Наукові праці, які засвідчують апробацію матеріалів дисертації:

5. Савлюк М. Інформаційна безпека в соціальних мережах: безпековий вимір для держави. *Публічне управління та адміністрування в Україні: Євроінтеграційний поступ:* збірник матеріалів ІІ Всеукраїнської науково-практичної конференції за міжнародної участі (м. Івано-Франківськ, 30 травня 2025 р.). Івано-Франківськ, 2025. С.101-104.

URL: https://nung.edu.ua/sites/default/files/2025-06/Збірник_тез_ІФНТУНГ_Т.2_2025_0.pdf

6. Савлюк М. Політика забезпечення інформаційної безпеки: міжнародний контекст. *Проблеми забезпечення інформаційної безпеки в міжнародному співробітництві*: матеріали міжнародної науково-практичної конференції, 5 вересня 2025 року. Ужгород, 2025. С.211-218.

7. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки як складник організаційно-правових засад функціонування системи безпеки критичної інфраструктури України. *Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення*. Збірник матеріалів І Міжнародної науково-практичної конференції (м. Івано-Франківськ, 27 листопада 2025 р.). Івано-Франківськ, 2025. С.199-202.

URL: https://nung.edu.ua/sites/default/files/2025-12/Збірник_тез_ІФНТУНГ_2025.pdf

8. Савлюк М. Сучасна протидія інформаційним загрозам: вітчизняний та світовий досвід. *Всеукраїнська науково-практична конференція здобувачів вищої освіти та молодих учених: Національна безпека України в умовах воєнного стану: проблеми та шляхи їх вирішення*: зб. матеріалів всеукраїнської наук.-практ. конф. (м. Одеса, 20 березня 2026 р.). Одеса: Військова академія, 2026. С.359-360.