АНОТАЦІЯ

Галіпчак В. Д. Інституційні чинники інформаційно-безпекової політики України в умовах воєнного стану. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 05 Соціальні та поведінкові науки за спеціальністю 052 Політологія, Прикарпатський національний університет імені Василя Стефаника, Івано-Франківськ, 2025.

Дисертаційне дослідження присвячене розв'язанню актуального теоретико-прикладного завдання – аналізу інституційних чинників інформаційно-безпекової політики в умовах воєнного стану.

Для сучасного світу притаманний динамічний розвиток інформаційних технологій (самобутні диджиталізаційні зміни), які, першоєю чергою, детерміновані зростанням ролі інформації в житті суспільства та держави. Останнє природно зумовлює потребу виформовування ефективних механізмів захисту інформаційного простору, що вкрай актуальне щодо збереження національної безпеки. Своєю чергою, особливої значущості набуває розгляд інституційних чинників інформаційно-безпекової політики, що пов'язане з стрижневою роллю останніх щодо підґрунтя, розвитку та реалізації стратегій захисту інформаційного простору країни.

Мовиться про те, що аналіз вищезазначених чинників репрезентативний не лише щодо наявних викликів та загроз, а й локалізації, ідентифікації тощо потенційних лакун, натомість врахування останніх продукує зміцнення інформаційної безпеки. Саме тому вибір теми дослідження базований на низці релевантних складників, побутування яких корелює з актуальністю та значущістю цього напряму дослідження на сьогодні. Зокрема:

а) *геополітичний контекст* (полягає у актуалізації таких елементів як діахронія (вертикальна локалізація стану інформаційної безпеки безвідносно до її попереднього контексту (трансформаційних змін, станів, специфіки), яка

полягає у аналізі тієї чи тієї параметризації на певному етапі: до прикладу, актуальний стан) і синхронія (горизонтальна локалізація – її суть у відстеженні динаміки генези такої безпеки з низкою причиново-наслідкових зв'язків: до прикладу: мовиться про врахування таких релеватних віх як анексія Криму, події на Сході України та широкомасштабне вторгнення країни-агресора, які зумовлюють не лише військову, а й інформаційну лінію фронту);

б) *збільшувана релевантність інформаційного простору* (йдеться про зростаючу роль даних щодо впливу на громадську думку (дезінформацію, мізінформацію, пропаганду тощо), формування тих чи тих наративів як складників самобутнього сторітеллінгу, нової міфології тощо, що, своєю чергою, стають частиною модерної ідеологічної полісистеми, метою якої є маніпулювання свідомістю громадян, а також роль інформаційно-безпекової політики як інструментарію боротьби з вищезазначеними виявами в контексті національної безпеки;

в) *лакунізованість аналізованої проблематики* (репрезентована дуальною природою останньої: з одного боку, спостерігаємо зростаючу роль проблем інформаційної безпеки, що зумовлює аналіз інституційних чинників, які релевантні щодо формування та реалізації вищезазначеної політики в нашій країні; з іншого – постулюємо відсутність комплексного підходу до вищезазначеного питання й потребу у синхронічному підході до нього, який продукуватиме актуалізацію наукового спадку і забезпечить органічність, питомість, адаптивність тощо продукованих кроків заради такої політики);

г) власне, *актуальність* (детермінована гібридною російсько-українською війною, яка позначена функціонуванням цілої низки неправдивих, викривлених тощо даних, що використовуються ворогом для дискредитації влади, ЗСУ, мобілізаційних заходів та іншого й протидія яким безпосередньо пов'язана з самобутністю актуалізації інституційних чинників у безпековій політиці сучасної України) й ґ) *глобалізаційний контекст* (полягає у інтеграції міжнародного досвіду (концепцій, практик, кампаній тощо) щодо інформаційно-безпекових ініціатив й адаптації ефективного

інструментарію задля протидії низці інформаційних загроз на українському підґрунті).

Актуальність теми дослідження зумовлена експонетним зростанням наявних викликів інформаційної безпеки, посилених російською агресією в Україні. Останнє спродукувало потребу у оперативному реагуванні її уряду на поточні загрози з вибудовуванням політичних концепцій, стратегій, практик тощо. Першою чергою, це пов'язане з формуванням стійкості інформаційного простору до можливих вразливостей у майбутньому й вибудовуванням сценаріїв протидії їм. Своєю чергою, актуальним також є вивчення параметризаційних особливостей в контексті генези наукових підходів до поняття інформаційної безеки та розробки ефективних стратегій її функціонування в умовах сучасних диджиталізаційних й геополітичних загроз.

Показово, що досліджені у науковій роботі теоретико-методологічні засади поняття національної безпеки у диджиталізаційному вимірі дозволяють здійснити глибокий аналіз інформаційної безпеки як геополітичної детермінанти (державності). Натомість глибокий аналіз безпеки інформаційного простору України з екстраполяцією сучасних викликів та міжнародного досвіду продукує вичленування самобутності українського контексту та виокремлення релевантних напрямів генези інформаційно-безпекової політики.

Отже, вибір теми дослідження детермінований не лише актуальністю аналізованої проблематики, а й потребою у випрацюванні ґрунтовного, комплексного й вичерпного підходу до побутування інформаційного простору України. Останній проаналізовано у межах дисертації в контексті гарантування сталого розвитку (стабільності, генези тощо) й безпеки (захисту, збереження та іншого). Своєю чергою, це продукує потребу у глибокому аналізі інституційних чинників й випрацювання ефективних стратегій щодо протидії наявним і потенційним загрозам для такого простору.

Метою роботи є комплексне та всебічне вивчення інституційних

аспектів формування та реалізації інформаційно-безпекової політики України, виявлення основних проблем та викликів, що стоять перед державою у цій сфері в контексті зовнішньої агресії, а також розробка рекомендацій щодо оптимізації інституційного механізму забезпечення інформаційної безпеки на базі кращих національних та міжнародних практик.

Об'єктом дослідження є інституційні чиннинки інформаційно-безпекової політики України в умовах зовнішніх загроз та впливів.

Предмет дослідження становлять процеси та закономірності формування й реалізації інформаційно-безпекової політики України з урахуванням міжнародного досвіду для боротьби проти російської агресії.

Досягнення вищезазначеної мети, об'єкта, предмета дисертаційної роботи відбулося шляхом розв'язання низки дослідницьких *завдань*:

– доповнити й систематизувати теоретико-методологічні засади дослідження поняття національної безпеки та її диджиталізаційний вимір у контексті інституційних чинників інформаційно-безпекової політики;

– висвітлити трансформаційні зміни категорійно-понятійного апарату інформаційно-безпекової політики України щодо його динаміки, специфіки тощо задля виокремлення кореляцій між поняттям національної та інформаційної безпеки;

– виокремити самобутню генезу поняття національних інтересів у диджиталізаційному вимірі, категоризувавши, структурувавши, вибудувавши за значущістю щодо зовнішніх / внутрішніх складників;;

– відстежити особливості побутування системи інформаційного простору, диференціюючи останню щодо функційної параметризації покладених на неї питомих завдань;

– сформулювати власне визначення поняття державно-правового механізму інформаційної безпеки, проаналізувавши джерельну (нормативно-правову базу) та оцінивши ефективність наявних моделей інформаційної безпеки;

– схарактеризувати сучасні виклики безпеці інформаційного простору

України в контексті параметризаційних особливостей розгортання гібридної російсько-української війни та інформаційної агресії, яка її супроводжує;

– екстраполювати міжнародний досвід західних держав-партнерів щодо інформаційного протистояння під час гібридних й інформаційних воєн;

– ідентифікувати види наявних та потенційних загроз, продукованих російською федерацією для України, задля формування рекомендацій до адаптації й імплементації вищезазначених практик, стратегій тощо.

У результаті проведеного дослідження здобувачем одержано такі наукові результати, зумовлені комплексним, ґрунтовним вивченням самобутності генези інституційних чинників інформаційно-безпекової політики України. Остання досліджена у корелятивному зв'язку з низкою викликів в умовах гібридної та інформаційної російсько-української війни. Зокрема, наукова робота заповнює такі лакуни у аналізованій проблематиці:

Уперше: а) комплексно досліджено підходи до розуміння інформаційної безпеки як складника національної безпеки держави й локалізовано роль і місце інституційних чинників у її функціонуванні; б) розроблено та обґрунтовано теоретичну модель інституційної взаємодії в царині інформаційної безпеки, яка враховує специфіку гібридної війни та потребу адаптації національної безпекової стратегії до змінюваних умов внутрішнього і зовнішнього середовища; в) опрацьовано широкий масив історіографії та репрезентативну джерельну базу з аналізованої проблематики задля відстеження генези інституційних чинників інформаційно-безпекової політики України та їх ролі у цьому процесі; г) запропоновано авторське визначення поняття національної безпеки та інформаційно-безпекової політики; г) ідентифіковано види наявних та потенційних загроз, продукованих російською федерацією для України, сформовано рекомендації до адаптації й імплементації практик, стратегій тощо вищезазначеної політики; д) проведено вивчення інформаційно-безпекових практик на основі SWOT-аналізу та методів прогнозування, що дозволило визначити ключові напрями оптимізації державної політики у цій царині.

Уточнено та вдосконалено: а) теоретико-методологічні засади дослідження поняття національної безпеки та її диджиталізаційний вимір у контексті інституційних чинників інформаційно-безпекової політики; б) категорійно-понятійний апарат такої політики щодо динаміки, специфіки тощо останнього задля виокремлення кореляцій між поняттям національної та інформаційної безпеки; в) особливості побутування системи інформаційного простору з диференціацією останньої щодо функційної параметризації покладених на неї питомих завдань.

Новий рівень отримали положення про: а) самобутню генезу поняття національних інтересів у диджиталізаційному вимірі щодо їх категоризації, структуризації та іншого з вибудовуванням за значущістю щодо зовнішніх/внутрішних складників й кореляцією з впливом законодавчих і нормативних документів на формування інформаційного простору України; б) роль інституційних чинників в процесі формування й реалізації інформаційно-безпекової політики в контексті міжнародного досвіду (інформаційного протистояння під час гібридних й інформаційних воєн) та виокремлення оптимальних моделей взаємодії між різними інституційними суб'єктами (включаючи державні органи, громадські інституції та міжнародні організації); в) ключові принципи та механізми міжнародної кооперації у галузі інформаційної безпеки, що може стати основою для розробки нових міжнародних договорів та угод, а також низки викликів безпеці інформаційного простору в контексті параметризаційних особливостей розгортання гібридної російсько-української війни й інформаційної агресії, яка її супроводжує.

Практичне значення роботи полягає у можливості використання її наукових здобутків у навчальному процесі (зокрема, лекційних, семінарських заняттях, контрольних роботах, іспитах тощо у закладах вищої освіти). Поза тим, дані дисертаційного дослідження можуть бути актуалізовані під час розробки навчальних курсів з низки політологічних, соціологічних та інших дисциплін. Зокрема, за такими напрямами підготовки як «Національна

безпека», «Політологія», «Міжнародні відносини», «Європейські студії», «Інформаційна безпека» та інші. Окрім того, його результати доцільно використати для створення навчальних підручників, посібників, методичних рекомендацій тощо, а також під час написання кваліфікаційних наукових праць. Результати наукового пошуку покликані сприяти подальшому розвитку та безпосередньому внеску в посилення національної безпеки України, формування стійкості інформаційного простору до зовнішніх та внутрішніх викликів, а також у забезпеченні сприятливих умов для розвитку інформаційного суспільства в країні.

Ключові слова: війна, воєнний стан, гібридна війна, дезінформація, діджиталізація, , інформаційна безпека, інформаційно-безпекова політика інформаційна політика, інформаційне суспільство, інформаційний простір, Європейський Союз, європейська інтеграція, національна безпека, політична комунікація, політична участь.

ABSTRACT

Galipchak V. D. Institutional factors of information and security policy of Ukraine in the conditions of martial law. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 05 Social and behavioral sciences with a specialty 052 Political Science, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, 2024.

The dissertation research is devoted to solving an urgent theoretical and applied task – analyzing the institutional factors of information and security policy under martial law.

The modern world is characterized by the dynamic development of information technologies (original digitalization changes), primarily determined by the growing role of information in society and the state. The latter naturally leads to the need to develop effective mechanisms for protecting the information space, which is extremely important for maintaining national security. In turn, the

consideration of institutional factors of information and security policy is of particular importance, which is related to the latter's pivotal role in the foundation, development, and implementation of strategies for protecting the country's information space.

The point is that the analysis of the above factors is representative not only of existing challenges and threats but also of localization, identification, etc. of potential gaps while considering that the latter leads to the strengthening of information security. That is why the choice of the research topic is based on several relevant components, the existence of which correlates with the relevance and importance of this area of research today. In particular:

a) *geopolitical context* (consists in the actualization of such elements as diachrony (vertical localization of the state of information security without regard to its previous context (transformational changes, states, specifics), which consists in the analysis of a particular parameterization at a certain stage: for example, the current state) and synchrony (horizontal localization - its essence is to track the dynamics of the genesis of such security with several cause-and-effect relationships: for example, it is about taking into account such relevant milestones as the annexation of Crimea, events in eastern Ukraine and the large-scale invasion of the aggressor country, which determine not only the military but also the information front line);

b) *the increasing relevance of the information space* (this refers to the growing role of data in influencing public opinion (disinformation, misinformation, propaganda, etc.), the formation of certain narratives as components of original storytelling, new mythology, etc., which, in turn, become part of a modern ideological poly system aimed at manipulating the consciousness of citizens, as well as the role of information and security policy as a tool to combat the above-mentioned manifestations in the context of national security;

c) *the lacunarity of the analyzed issues* (represented by the dual nature of the latter): on the one hand, we observe the growing role of information security issues, which leads to the analysis of institutional factors relevant to the formation and

implementation of the above policy in our country; on the other hand, we postulate the lack of a comprehensive approach to the above issue and the need for a synchronous approach to it, which will produce an actualization of the scientific heritage and ensure the organicity, specificity, adaptability, etc. of the steps taken for such a policy);

d) *actual relevance* (determined by the hybrid russian-Ukrainian war, which is marked by the functioning of several false, distorted, etc. data used by the enemy to discredit the government, the Armed Forces of Ukraine, mobilization activities, etc., and counteracting them is directly related to the originality of the actualization of institutional factors in the security policy of modern Ukraine); and g) the globalization context (involves the integration of international experience (concepts, practices, campaigns, etc.) in information and security initiatives and the adaptation of effective tools to counter several information threats on Ukrainian soil).

The relevance of the research topic is due to the exponential growth of existing information security challenges, exacerbated by russian aggression in Ukraine. The latter has created a need for the government to respond promptly to current threats by developing political concepts, strategies, practices, etc. First of all, this is related to the formation of the information space's resilience to possible future vulnerabilities and the development of scenarios to counter them. In turn, it is also relevant to study parameterization features in the context of the genesis of scientific approaches to the concept of information security and the development of effective strategies for its functioning in the context of modern digitalization and geopolitical threats.

It is noteworthy that the theoretical and methodological foundations of the concept of national security in the digitalization dimension studied in the research paper allow for an in-depth analysis of information security as a geopolitical determinant (statehood). In turn, a deep analysis of the security of Ukraine's information space with extrapolation of modern challenges and international experience produces a distinction between the identity of the Ukrainian context and the identification of relevant areas of the genesis of information and security policy.

Thus, the choice of the research topic is determined not only by the relevance of the analyzed issues but also by the need to develop a thorough, comprehensive, and exhaustive approach to the existence of the information space of Ukraine. The latter is analyzed in this thesis in the context of ensuring sustainable development (stability, genesis, etc.) and security (protection, preservation, etc.). In turn, this creates the need for an in-depth analysis of institutional factors and the development of effective strategies to counteract existing and potential threats to such a space.

The purpose of the study is to comprehensively and comprehensively study the institutional aspects of the formation and implementation of Ukraine's information and security policy, identify the main problems and challenges facing the state in this area in the context of external aggression, and develop recommendations for optimizing the institutional mechanism for ensuring information security based on the best national and international practices.

The object of the study is the institutional factors of Ukraine's information and security policy in the context of external threats and influences.

The subject of the study is the processes and patterns of formation and implementation of Ukraine's information and security policy, taking into account international experience, to combat russian aggression.

Achievement of the above goal, object, and subject of the dissertation was achieved by solving several research *tasks*:

– to supplement and systematize the theoretical and methodological foundations of the study of the concept of national security and its digitalization dimension in the context of institutional factors of information and security policy;

– to highlight the transformational changes in the categorical and conceptual apparatus of the above-mentioned policy in terms of dynamics, specificity, etc. of the latter to highlight the correlations between the concepts of national and information security;

– to distinguish the original genesis of the concept of national interests in the digitalization dimension and to categorize, structure, etc., arranging it by importance in terms of external/internal components;

– to trace the peculiarities of the information space system, differentiating the latter in terms of functional parameterization of its specific tasks;

– to study and formulate the author's definition of the concept of the state-legal mechanism of information security, analyzing the source (regulatory framework) and evaluating the effectiveness of existing models of the latter;

– to analyze current challenges to the security of Ukraine's information space in the context of the parameterization features of the deployment of the hybrid russian-Ukrainian war and the information aggression that accompanies it;

– extrapolate the international experience of Western partner states in information confrontation during hybrid and information wars;

– to identify the types of existing and potential threats posed by the Russian Federation to Ukraine to formulate recommendations for the adaptation and implementation of the above practices, strategies, etc.

As a result of the study, the applicant obtained the following scientific results, which are due to a comprehensive, thorough study of the originality of the genesis of institutional factors of Ukraine's information and security policy. The latter is studied in correlation with several challenges in the context of the hybrid and information russian-Ukrainian war. In particular, the scientific work fills the following gaps in the analyzed issues:

For the first time: a) approaches to understanding information security as a component of the national security of the state are comprehensively studied and the role and place of institutional factors in its functioning are localized; b) developed and substantiated a theoretical model of institutional interaction in the field of information security is developed and substantiated, which takes into account the specifics of hybrid warfare and the need to adapt the national security strategy to changing conditions of the internal and external environment; c) a wide range of historiography and a representative source based on the analyzed issues were processed to trace the genesis of institutional factors of Ukraine's information and security policy and their role in this process; d) the author's definition of the concept of national security and information and security policy was proposed on the above

basis; e) the types of existing and potential threats posed by the Russian Federation to Ukraine were identified, recommendations for the adaptation and implementation of practices, strategies, etc. of the above-mentioned.

The author clarifies and improves: a) the theoretical and methodological foundations of the study of the concept of national security and its digitalization dimension in the context of institutional factors of information and security policy; b) the categorical and conceptual apparatus of such a policy regarding the dynamics, specificity, etc. of the latter to highlight the correlations between the concepts of national and information security; c) the peculiarities of the information space system with the differentiation of the latter in terms of the functional parameterization of its specific tasks.

A new level was given to the provisions on: a) the original genesis of the concept of national interests in the digitalization dimension in terms of their categorization, structuring, etc. with the alignment of importance in terms of external/internal components and correlation with the impact of legislative and regulatory documents on the formation of the information space of Ukraine; b) the role of institutional factors in the process of forming and implementing information and security policy in the context of international experience (information confrontation during hybrid and information wars) and the identification of optimal models of interaction between different institutional actors (including government agencies, public institutions and international organizations); c) key principles and mechanisms of international cooperation in the field of information security, which can become the basis for the development of new international treaties and agreements, as well as several challenges to the security of the information space in the context of the parametrization features of the hybrid russian-Ukrainian war and the information aggression that accompanies it.

The practical significance of the study lies in the possibility of using its scientific achievements in the educational process (in particular, lectures, seminars, tests, exams, etc. in higher education institutions). In addition, the data of the dissertation research can be actualized in the development of training courses in

several political science, sociology, and other disciplines. In particular, in such areas of training as “National Security”, “Political Science”, “International Relations”, “European Studies”, “Information Security” and others. In addition, its results can be used to create textbooks, manuals, guidelines, etc., as well as in writing scientific research (term papers, diploma papers, master’s, PhD, and doctoral dissertations). Also, the materials of the scientific work are intended to contribute to the further development and direct contribution to strengthening the national security of Ukraine, building the resilience of the information space to external and internal challenges, as well as to ensuring favorable conditions for the development of the information society in the country.

Key words: war, martial law, hybrid war, disinformation, digitalization, information security, information security policy, information policy, information society, information space, European Union, European integration, national security, political communication, political participation.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Галіпчак В. Інформаційна війна як складова гібридної війни в умовах російьскої агресії. *Вісник Прикарпатського університету. Політологія.* 2023. №15. С. 26-32.

DOI: https://doi.org/10.32782/2312-1815/2024-1-4

URL: http://politicus.od.ua/index.php/2023-ukr?id=64

2. Галіпчак В. Інституційні чинники інформаційної політики євроінтеграції України: безпековий вимір. *Політикус.* 2023. №3. С. 97-102.

DOI https://doi.org/10.24195/2414-9616.2023-3.17

URL: http://politicus.od.ua/index.php/2023-ukr?id=64

3. Галіпчак В. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Науковий журнал «Регіональні студії»,* 2023. №34. С. 81-85.

DOI https://doi.org/10.32782/2663-6170/2023.34.13

URL: http://regionalstudies.uzhnu.uz.ua/index.php/34

4. Галіпчак В. Трансформація інформаційного простору України під впливом російськоїагресії: зміни та виклики. *Політикус.* 2023. №4. С. 26-31.

DOI https://doi.org/10.24195/2414-9616.2023-4.4

URL: http://politicus.od.ua/index.php/2023-ukr?id=65

5. Галіпчак В. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. *Політикус.* 2023. №5. С. 19-24.

DOI https://doi.org/10.24195/2414-9616.2023-5.3

URL: http://politicus.od.ua/index.php/2023-ukr?id=66

6. Галіпчак В. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії: перспективи та завдання. *Науковий журнал «Регіональні студії».* 2023. №35. С. 65-70.

DOI https://doi.org/10.32782/2663-6170/2023.35.10

URL: http://regionalstudies.uzhnu.uz.ua/index.php/35

Статті у періодичних наукових виданнях інших держав, включених до міжнародних наукометричних баз Scopus/Web of Science:

7. Slobodianiuk A., Vonsovych S., Bezerovska-Chmil O., Nykorovych Y., Halipchak V. Political aspects of decision-making . *AD ALTA: Journal of Interdisciplinary Research. Web of Science. The Czech Republic.* 2023. Volume 13. Issue 2. Page 23-26.

URL: https://www.magnanimitas.cz/ADALTA/130236/papers/A_04.pdf

Список публікацій здобувача, які додатково відображають наукові результати дисертації:

8. Галіпчак В. Здійснення інформаційної політики євроінтеграції. Безпека інформаційного суспільства ЄС. *Прикарпатський вісник НТШ. Думка.* 2021. №5. С. 21-24.

URL:https://pnu.edu.ua/wp-content/uploads/2021/04/Програма-звітної-конференції-викладачів-за-2020-рік-2.pdf

9. Галіпчак В. Державно правовий механізм забезпечення інформаційної безпеки. *Матеріали ІІІ Всеукраїнської науково-практичної конференції «Політичні процеси сучасності: глобальний та регіональний вимір» (м.Івано-Франківськ, 27-28 травня 2021р.).* Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2021.

URL:https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/56376/1/Збірник%20Конференції%2027-28%20травня%202021%20%28Івано-Франківськ%29.pdf

10. Галіпчак В. Основні методологічні засади поняття національної безпеки: інформаційий вимір. *POLITIA. Вісник наукових робіт молодих вчених.* Івано-Франківськ: ЯРИНА, 2023. Вип. 5. С. 192–225.

URL:https://kpip.pnu.edu.ua/wp-content/uploads/sites/121/2023/04/politia-5.pdf

11. Галіпчак В. Державно-правовий механізм здійснення інформаційної безпеки: агенти і методи впливу. *Матеріали Всеукраїнської науково-практичної конференції « Теоретичні та практичні аспекти політичного розвитку в Україні і світі в умовах повномасштабної російсько-української війни (пам'яті Любомири Мандзій)» (м.Львів, 10 травня 2023р.).* Львів: Львівський національний університет імені Івана Франка, 2023. С. 40-42.

URL:https://filos.lnu.edu.ua/wpcontent/uploads/2023/05/Conf_Program_May23.pdf

12. Галіпчак В. Роль інституційних механізмів у запезпеченні інформаційної безпеки: аспекти управління та взаємодії. *IX Міжнародна науково-практична конференція «Практичні та теоретичні питання розвитку науки та освіти» (м. Львів, 29-30 жовтня 2023 року).* Львів: Львівський науковий форум, 2023р. С. 35-37.

URL:http://www.lviv-forum.inf.ua/save/2023/29-30.10/Збірник.pdf

13. Галіпчак В. Вплив інформаційних технологій на захист національних інтересів в Україні: виклики та можливості. *X Міжнародна науково-практичніа конференція «Пріоритетні шляхи розвитку науки і освіти» (м. Львів, 29-30 листопада 2023 року).* Львів: Львівський науковий форум, 2023р. С. 70-73.

URL:http://www.lviv-forum.inf.ua/save/2023/29-30.11/Збірник.pdf