ISSN 2076–1554

Український державний університет
імені Михайла Драгоманова

Видавництво «Гілея»

Гілея

Науковий вісник

Випуск 205-206 (№ 3-4)

Київ – 2025

ISSN 2076–1554

Збірник засновано 2004 року. Вихід з друку – щомісячно

Реєстрація в Національній раді України з питань телебачення і радіомовлення: Витяг з реєстру суб'єктів у сфері медіа-реєстрантів. Ідентифікатор медіа R30-04516 (рішення No 2694 від 05.09.2024 року)

Друкується за рішенням:

Вченої ради Українського державного університету ім. Михайла Драгоманова

(протокол № 09 від 24 квітня 2025 р.)

Збірник входить до міжнародних баз

Google Scholar; Index Copernicus (Польща); EBSCO Publishing, Inc. (USA); SIS (Scientific Indexing Services) (USA); InfoBase Index (Індія).

Шеф – редактор:

Андрущенко В. П., д–р філос. наук, проф., член-кореспондент НАН України, академік НАПН України (Український державний університет ім. Михайла Драгоманова)

Головний редактор:

Вашкевич В. М., д–р філос. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Відповідальний редактор:

Іванець Н. В., доктор філософії PhD, завідувачка Навчально-наукової лабораторії «Соціальна філософія, філософія освіти та освітня політика» (Український державний університет імені Михайла Драгоманова)

Редакційна рада:

Андрущенко В. П., д–р філос. наук, проф., член-кореспондент НАН України, академік НАПН України (Україна, Український державний університет імені Михайла Драгоманова)

Вашкевич В. М., д–р філос. наук, проф. (Україна, Український державний університет імені Михайла Драгоманова)

Гуменюк Б. І., д–р іст. наук, проф. (Україна, Український державний університет імені Михайла Драгоманова)

Куйбіда В. С., д-р наук з державного управління, кандидат юридичних наук, проф., (Україна, президент Всеукраїнської асоціації магістрів державного управління)

Рафальський О. О., д–р іст. наук, проф., академік НАН України, академік НАПН України (Україна, Інститут політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України, Віце-президент НАН України)

Солдатенко В. Ф., д–р іст. наук, проф., член-кореспондент НАН України (Україна, Інститут політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України)

Редакційна колегія з філософських наук:

Вашкевич В. М., д–р філос. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Глушко Т. П., д–р філос. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Драпушко Р.Г., канд. філос. наук, доц. (Український державний університет ім. Михайла Драгоманова)

Жижко Т. А., д–р філос. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Кивлюк О. П., д–р філос. наук, проф. (Київського університету інтелектуальної власності та права Національного університету «Одеська юридична академія»)

Панченко Л. М., канд. філос. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Шиндаулова Раушан, д-р філос. наук (Казахстан, Казахська національна консерваторія імені Курмангази)

Ярошенко А. О., д–р філос. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Редакційна колегія з політичних наук і публічного управління та адміністрування:

Андрущенко Т. В., д–р політ. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Андрюкайтене Р., д-р PhD соціальних наук (менеджмент), (Литва, Маріямполь)

Бебик В. М., д–р політ. наук, канд. психологічних наук, проф. (Український державний університет ім. Михайла Драгоманова)

Древаль Ю. Д., д-р наук з державного управління, проф. (Національний університет цивільного захисту України, Харків)

Котигоренко В. О., д–р політ. наук, проф. (Україна, Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України)

Куйбіда В. С., д-р наук з державного управління, канд. юридичних наук, проф., (Україна, президент Всеукраїнської асоціації магістрів державного управління)

Новакова О. В., д–р політ. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Тімашова В. М., д-р політ. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Редакційна колегія з історичних наук:

Андрусишин Б. І., д–р іст. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Гуменюк Б. І., д–р іст. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Євтух В. Б., д–р іст. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Лучаківська Ів., доктор філософії, доц. (Жешувський Університет, (Польща)

Макарчук С. С., канд. іст. наук, доц., керівник (Миколаїв, Обласний центр пошукових досліджень та редакційно-видавничої діяльності)

Мелещенко Т. В., канд. іст. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Потильчак О. В., д–р іст. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Стоян Т. А., д–р іст. наук, проф. (Український державний університет ім. Михайла Драгоманова)

Гілея: науковий вісник. – К. : «Видавництво «Гілея», 2025. – Вип. 205-206 (№ 3-4). – 149 с.

Концепція збірника базується на багатоплановому науковому висвітленні проблем сучасної науки в умах полікультурного глобалізаційного суспільства. Основні рубрики охоплюють галузі історичних, філософських та політичних наук. Розрахований на фахівців гуманітарних та соціально-політичних наук.

© Редакційна колегія, 2025
© Автори статей, 2025
©Український державний університет імені Михайла Драгоманова, 2025

ISSN 2076-1554

Ukrainian State University named after
Mykhailo Drahomanov

Publishing House Hileya

Hileya

SCIENTIFIC BULLETIN

Volume 205-206 (№ 3-4)

Kyiv – 2025

ISSN 2076–1554

The collection is founded in 2004. Printed on a monthly basis

Certificate of printed mass media's state registration (re-registration):Series КВ № 22632-12532ПР from April 17th, 2017

Printed by decision
of Ukrainian State University named after Mykhailo Drahomanov
(protocol № 09 of April24, 2025)

The collection is a member of international database
Google Scholar; Index Copernicus (Poland); EBSCO Publishing. Inc. (USA),SIS (Scientific Indexing Services) (USA); InfoBase Index (India).

Honored Chief Editor:

Andrushchenko V. P., Doctor of Philosophical Sciences, Professor, Corresponding Member of NASU, Acad. of NAPS Ukraine (Ukrainian State University named after Mykhailo Drahomanov)

Chief Editor:

Vashkevych V. M., Doctor of Philosophical Sciences, Professor, (Ukrainian State University named after Mykhailo Drahomanov)

Editor-in-Chief:

Responsible editor: Ivanets N. V., Ph.D. Sciences, Head of the Educational and Scientific Laboratory "Social Philosophy, Philosophy of Education and Educational Policy" (Ukrainian State University named after Mykhailo Drahomanov)

Editorial Board:

Andrushchenko V. P., Doctor of Philosophy Science, Prof., Member - cor. NAS of Ukraine, Acad. National Academy of Sciences of Ukraine (Ukraine, Ukrainian State University named after Mykhailo Drahomanov)

Vashkevich V. M., Doctor of Philosophy Sciences, Prof. (Ukraine, Mykhailo Drahomanov Ukrainian State University)

Humenyuk B. I., Doctor of History Sciences, Prof. (Ukraine, Mykhailo Drahomanov Ukrainian State University)

Kuybida V. S., Doctor of Public Administration, Candidate of Sciences. of Legal sciences, Prof., (Ukraine, president of the All-Ukrainian Association of Masters of Public Administration)

Rafalskyi O. O., Doctor of History, Sciences, Prof., Acad. National Academy of Sciences of Ukraine (Ukraine, I. F. Kuras Institute of Political and Ethnonational Studies of the National Academy of Sciences of Ukraine)

Soldatenko V.F., Doctor of History Sciences, Prof., Member-cor. National Academy of Sciences of Ukraine (Ukraine, I.F. Kuras Institute of Political and Ethnonational Studies, National Academy of Sciences of Ukraine)

Philosophical Sciences Editorial Board:

Vashkevich V. M., Doctor of Philosophy. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Hlushko T. P., Doctor of Philosophy. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)
Drapushko R. G., Candidate of Philosophical Sciences, Associate Professor (Mykhailo Dragomanov Ukrainian State University)

Zhizhko T. A., Doctor of Philosophy. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Kyvlyuk O. P., Doctor of Philosophy. Sciences, Prof. (Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy")

Panchenko L. M., candidate Philos. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Shindaulova Raushan, Doctor of Philosophy. Sciences (Kazakhstan, Kazakh National Conservatory named after Kurmangazy)

Yaroshenko A. O., Doctor of Philosophy. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Editorial board for political sciences and public management and administration:

Andrushchenko T. V., Doctor of Aviation. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Andryukaitene R., PhD, Social Sciences (Management), (Lithuania, Marijampol)

Bebyk V. M., Doctor of Aviation. of Science, candidate of psychological sciences, prof. (Ukrainian State University named after Mykhailo Drahomanov)
Dreval Yu. D., Doctor of Public Administration, Professor (National University of Civil Defense of Ukraine, Kharkiv)

Kotyhorenko V. O., Doctor of Aviation. Sciences, Prof. (Ukraine, I.F. Kuras Institute of Political and Ethnonational Studies of the National Academy of Sciences of Ukraine)

Kuybida V. S., Doctor of Public Administration, Candidate of Sciences. of legal sciences, prof., (Ukraine, president of the All-Ukrainian Association of Masters of Public Administration)

Novikova O. V., Doctor of aviation. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Timashova V. M., Doctor of aviation. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Editorial board for historical sciences:

Andrusyshyn B. I., Ph.D. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Humenyuk B. I., Doctor of History Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Yevtukh V. B., Doctor of History Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Luchakivska Iv., Ph.D. Sciences, associate professor (University of Rzeszów, (Poland)

Makarchuk S. S., candidate history of Sciences, associate professor, manager (Mykolaiv, Regional Center for Search Research and Editorial and Publishing Activity)

Meleshchenko T. V., candidate history Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Potylchak O. V., Doctor of History Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Stoyan T. A., Ph.D. Sciences, Prof. (Ukrainian State University named after Mykhailo Drahomanov)

Hileya: Scientific Bulletin. – Kyiv : «Publishing house «Hileya», 2025. – Volume 205-206 (№ 3-4). – 149 p.

The collections' concept is based on a multifaceted scientific coverage of the problems of formation of informational civilization. The main headings cover areas of historical, philosophical and political sciences. It is designed for specialists in the humanities and socio-political sciences.

©Editorial board, 2025
©Authors of articles, 2025
© Ukrainian State University named after Mykhailo Drahomanov,2025

ПРЕДСТАВНИЦТВА
збірника «Гілея: науковий вісник» в Україні

Вінницьке представництво
(Вінницький національний технічний університет)
керівник **Денисюк С. Г.,** доктор політичних наук, професор
e–mail: svetadenisiyk@gmail.com

Дніпрівське представництво
(Дніпропетровський національний університет
імені Олеся Гончара)
керівник **Вершина В. А.,** кандидат філософських наук, доцент
e–mail: vivi.dp@ukr.net

Запорізьке представництво
(Запорізький національний технічний університет)
керівник **Ємельяненко Є. О.,** кандидат філософських наук, доцент
e–mail: gileya_zaporizhzhya@ukr.net

Івано–Франківське представництво
(Прикарпатський національний університет
імені Василя Стефаника, м. Івано–Франківськ)
керівник **Дзвінчук Д. І.,** доктор філософських наук, професор
e–mail: fuid@ua.fm

Київське представництво
(Інститут права і сучасних технологій Київського національного
університету технології та дизайну)
керівник **Дорошенко В. С.,** доктор наук з державного управління,
доцент
e – mail: vladimirdoroshenkosinger@gmail.com

Луганське представництво
(Східноукраїнський національний університет
імені Володимира Даля, м. Сєвєродонецьк)
керівник **Михайлюк В. П.,** доктор історичних наук, професор
e–mail: vital_mih@ukr.net

Миколаївське представництво
(Миколаївський національний університет
імені В. О. Сухомлинського)
керівник **Шкуренко К. О.,** кандидат політичних наук, доцент
e–mail: sh_kamila@mail.ru

Одеське представництво
(Одеський національний університет імені І. І. Мечникова)
керівник **Барвінська П. І.,** кандидат історичних наук, доцент
e–mail: barwinskaja@ua.fm

Подільське представництво
(Подільський державний аграрно–технічний університет,
м. Кам'янець–Подільський)
керівник **Колосюк І. А.,** кандидат філософських наук, доцент
e–mail: ikolosyuk@ukr.net

Полтавське представництво
(Полтавський факультет Національної юридичної академії
України ім. Ярослава Мудрого)
керівник **Куцепал С. В.,** доктор філософських наук, професор
e–mail: svkutsepal@rambler.ru

Сумське представництво
(Сумський державний університет)
керівник **Дегтярьов С. І.,**
доктор історичних наук, професор
e–mail: starsergo@bigmir.net

Тернопільське представництво
(Тернопільський національний педагогічний університет
імені Володимира Гнатюка)
керівник **Кліш А. Б.,** кандидат історичних наук, доцент
e–mail: Klish_Andriy@ukr.net

Ужгородське представництво
(Ужгородський національний університет)
керівник **Мелеганич Г. І.,** кандидат політичних наук, доцент
e–mail: melgi@ukr.net

Уманське представництво
(Уманський державний педагогічний університет
імені Павла Тичини)
керівник **Кривошея І. І.,** кандидат історичних наук, доцент
e–mail: igorkryvosheia@gmail.com

Харківське представництво
(Національний технічний університет
«Харківський політехнічний інститут»)
керівник **Владленова І. В.,** доктор філософських наук, професор
e–mail: vladlenova@email.ua

Хмельницьке представництво
(Хмельницький національний університет)
керівник **Гоцуляк В. М.,** кандидат політичних наук, доцент
e–mail: gotsylak@ukr.net

Черкаське представництво
(Черкаський національний університет
імені Богдана Хмельницького)
керівник **Васильчук Є. О.,** доктор політичних наук, доцент
e–mail: vasilchuk84@bk.ru

Чернігівське представництво
(Національний університет «Чернігівський колегіум»
імені Т. Г. Шевченка)
керівник **Костирєв А. Г.,** кандидат політичних наук, доцент
e–mail: akostyrev@ukr.net

ПРЕДСТАВНИЦТВО
збірника «Гілея: науковий вісник» в Азербайджані

(Національна Академія Наук Азербайджану, м. Баку)
керівник **Махмудов М. А.,** доктор філософії
e–mail: matlabm@yandex.com

ПРЕДСТАВНИЦТВА
збірника «Гілея: науковий вісник» в Польщі

(Університет імені Адама Міцкевича в Познані)
керівник **Димчик Р.,** доктор, викладач
e–mail: dymczyk@wp.pl

(Інститут історії Академії імені Яна Длугоша в Ченстохові)
керівник **Моравец Н.,** доктор, викладач
e–mail: mornor@wp.pl

Запрошуємо Вас відвідати наш сайт: **www.gileya.org**
E–mail: gileya.org.ua@gmail.com
Див. також: Сайт Національної бібліотеки України
імені В. І. Вернадського: www.nbuv.gov.ua/portal
Розділ: Наукова періодика України: журнали та збірники наукових праць

DOI:https://doi.org/10.31392/Hileya-POLITICAL-2025.205-206(3-4).09
УДК 351.746.1:001.102]:316.3

НАЦІОНАЛЬНА БЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

NATIONAL SECURITY IN THE INFORMATION SOCIETY

Дмитренко С. П.,
кандидат політичних наук,
доцент кафедри історії
міжнародних відносин та гуманітарних
дисциплін, Український державний
університет імені Михайла Драгоманова
(Україна, Київ)
e-mail: s.dmytrenko@udu.edu.ua
ORCID:https://orcid.org/ 0009-0005-4163-0468

Дмитренко О. С.,
кандидат політичних наук,
доцент кафедри історії
міжнародних відносин та гуманітарних
дисциплін, Український державний
університет імені Михайла Драгоманова
(Україна, Київ)
e-mail: o.dmytrenko@udu.edu.ua
ORCID:https://orcid.org/ 0009-0000-7621-2710

Dmitrenko S. P.,
candidate of Political Science, Associate Professor of the Department of History international relations and humanities Ukrainian State University named after Mikhail Drahomanov (Ukraine, Kyiv)
e-mail: s.dmytrenko@udu.edu.ua
ORCID:https://orcid.org/ 0009-0005-4163-0468

Dmitrenko O. S.,
candidate of Political Science, Associate Professor of the Department of History international relations and humanities Ukrainian State University named after Mikhail Drahomanov (Ukraine, Kyiv)
e-mail: o.dmytrenko@udu.edu.ua
ORCID:https://orcid.org/ 0009-0000-7621-2710

Розвідка репрезентує дослідження ключових аспектів нацбезпеки у розрізі поняття інформаційного суспільства. Автори розглянули пропаганду, витоки інформації, технологічну залежність, кібератаки, інформаційні війни як основні загрози цифрового простору, що підривають національну безпеку держави. Стратегічним ресурсом, який визначає розвиток будь-якої держави економіки та суспільства, є інформація.

Цифровізаційні та глобалізаційні процеси набувають критичного значення, оскільки Інтернет та соціальні медіа створюють нові можливості поширення цифрових технологій, а відтак і нові можливості серйозних загроз.

Актуалізація питання нацбезпеки в умовах російсько-української війни має масштабні виклики, що породжуються кібератаками, маніпуляціями та пропагандою.

Автори аналізують вплив суспільства інформації на нацбезпеку та визначають основні загрози. Інформаційне суспільство як феномен є формувачем соціальних і політичних процесів. Глобалізація взаємодії мережевих комунікацій через кібератаки, маніпуляції, втручання у внутрішні справи, шантаж на рівні інформації посилюють виклики національної безпеки, відтак, усе менш ефективними стають традиційні механізми захисту інформаційного суспільства та рівнів національної безпеки.

На цій підставі виникає потреба у розробці нових підходів та адаптивних умов розвитку безпеки у цифровій епосі.

Методологічною основою розвідки став системний аналіз, контент-аналіз інформаційних воєн, прогностичні методи та компаративний аналіз.

У статті побіжно окреслено практики забезпечення інформаційної безпеки, у тому числі Китаю, ЄС та США.

Інформаційна безпека, кібербезпека, політична безпека, культурна безпека є проаналізованими основними компонентами нацбезпеки в інформаційному суспільстві.

Особливу увагу автори звертають на вплив цифрових технологій та рівень державного управління, соціальну стабільність, економіку, належне регулювання кіберпростору, пропаганду нацбезпеки та розвиток аудиту дезінформаційних візій.

Автори опираються на вивчення ролі штучного інтелекту та стверджують, що посилення захисту інформаційного простору держави може бути забезпечене автоматизованими системами аналізу даних.

Для виявлення загроз у реальному часі, аналізу джерел інформації та боротьби з дезінформацією необхідно виробити законодавчу ініціативу у сфері регулювання інформаційної безпеки.

Гальмування цих процесів в Україні породжене відсутністю єдиної державної стратегії кіберзахисту, недостатнім рівнем фінансуванням та відсутністю кваліфікованих фахівців.

Стаття надає рекомендації щодо посилення нацбезпеки інформаційного суспільства, інтеграції штучного інтелекту, підвищення рівня медіаграмотності.

У подальших наукових розвідках автори будуть зосереджуватися на аналізі психологічних аспектів інформаційної безпеки та розробці візії стратегії задля протидії гібридним загрозам, а також створення єдиної національної екосистеми кібербезпеки та кіберзахисту.

Ключові слова: національна безпека, інформаційне суспільство, кібербезпека, інформаційні загрози, пропаганда.

The study explores key aspects of national security in the context of the information society. The authors examine propaganda, information leaks, technological dependence, cyberattacks, and information wars as primary threats in the digital space that undermine a state's national security. Information is identified as a strategic resource that determines the development of any state, its economy, and society.

Digitalization and globalization processes are becoming critically important, as the Internet and social media create new opportunities for the spread of digital technologies, which, in turn, lead to new serious threats.

The issue of national security has been particularly relevant in the context of the Russian-Ukrainian war, posing large-scale challenges such as cyberattacks, manipulations, and propaganda.

The authors analyze the impact of the information society on national security and identify key threats. The information society, as a phenomenon, shapes social and political processes. The globalization of network communications, through cyberattacks, manipulations, interference in internal affairs, and information blackmail, exacerbates national security challenges, rendering traditional protection mechanisms less effective in safeguarding the information society and national security levels.

This underscores the need to develop new approaches and adaptive security measures for the digital era.

The methodological foundation of the study includes systemic analysis, content analysis of information wars, predictive methods, and comparative analysis.

The article briefly outlines information security practices, including those of China, the EU, and the USA.

Information security, cybersecurity, political security, and cultural security are analyzed as the main components of national security in the information society.

The authors pay special attention to the influence of digital technologies on governance, social stability, the economy, proper cyber regulation, propaganda in national security, and the development of disinformation audit mechanisms.

The study emphasizes the role of artificial intelligence, arguing that enhancing the protection of a state's information space can be achieved through automated data analysis systems.

To detect threats in real-time, analyze information sources, and combat disinformation, it is necessary to develop legislative initiatives in the field of information security regulation.

In Ukraine, the delay in these processes is caused by the absence of a unified state cybersecurity strategy, insufficient funding, and a lack of qualified specialists.

The article provides recommendations for strengthening national security in the information society, integrating artificial intelligence, and improving media literacy.

Future research will focus on analyzing the psychological aspects of information security, developing strategic visions to counter hybrid threats, and creating a unified national cybersecurity and cyber defense ecosystem.

***Keywords**: national security, information society, cybersecurity, information threats, propaganda.*

Постановка проблеми у загальному вигляді та зв'язок із важливими науково-практичними завданнями. Визначення візії розвитку держави суспільства та економіки у сучасному світі взяла на себе інформація, яка має характеристики основного стратегічного ресурсу. Нових вимірів набуває національна безпека в контексті поширення цифрових технологій. За рахунок глобалізації через мережу Інтернет та соціальні медіа, а також створення як нових можливостей, так і серйозних загроз в інформаційному суспільстві, утворюється ознака домінування інформаційних технологій. Кібератаки, маніпуляції громадською думкою, втручання у внутрішні справи держав, інформаційний шантаж є різними формами та варіантами загроз інформаційній безпеці.

Україна в умовах українсько-російської війни гостро актуалізує це питання, оскільки саме інформаційна війна стає ключовим інструментом агресії. Забезпечення національної безпеки ґрунтується на трансформації суспільства під впливом цифровізації, відтак потребує нового підходу.

Сучасна наукова думка відзначає, що традиційні способи захисту державних інтересів є слабкими в контексті впливу на них сучасних інформаційних загроз. На цій підставі виникає необхідність досліджувати вплив інформаційних технологій на розвиток системи національної безпеки, а також аналізувати ключові загрози і розробляти ефективні механізми їх попередження та протидії.

Аналіз останніх досліджень та публікацій. Питання безпеки перебуває в центрі уваги багатьох науковців протягом багатьох років, включаючи істориків, юристів, філософів, політиків, державних діячів та військових. Розвідувально-підривна, терористична та гібридна військова діяльність росії проти України покладає на СБУ та українські спецслужби завдання найбільш ефективного забезпечення зовнішньополітичного курсу та національної безпеки держави [2, с. 186].

На сучасному етапі розвитку Україна стикається зі складними проблемами, пов'язаними з серйозними викликами щодо її суверенітету, і питання національної безпеки є критично важливим. Виклики останніх років підтверджують необхідність своєчасного аналізу загроз та якісної оцінки стану національної безпеки [8, с. 47]. Для України такий процес є критично важливим в умовах викликів з боку сусідніх держав-агресорів. В умовах військової агресії, геополітичних змін та внутрішніх реформ державна безпека є не лише гарантією суверенітету, а й основою стабільного сус-

пільного розвитку.

Усвідомлюючи безпекові реалії, держави можуть не лише ефективно реагувати на поточні загрози, а й стратегічно планувати майбутнє, забезпечувати захист національних інтересів, ставати менторами у розвитку нацбезпеки інших держав. Таким чином, оцінка національної безпеки є ключовим елементом у забезпеченні стійкості та розвитку України на міжнародній арені.

Необхідність захисту від загроз і небезпек зумовлює використання різних інструментів у сфері суспільних відносин, одним з яких є право, що є засобом координації державних політик [9, с. 7]. Незважаючи на послідовний розвиток безпекового права, питання змісту базової правової категорії «національна безпека» залишається невирішеним. У загальному викладі під державною безпекою [5, с. 156] як однією з головних умов нормального розвитку суспільства розуміється стратегічна [10, с. 49] захищеність якісного стану суспільних відносин, що гарантує прогресивний розвиток у певних історичних умовах, від небезпек, що виникають внаслідок внутрішніх і зовнішніх суперечностей [1, с. 1].

Категорія «національна безпека» є ширшою за категорію «державна безпека» і є важливим показником демократичності політичної системи конкретної держави. Тип політичної системи держави є дуже важливим для розмежування понять «національна безпека» і «державна безпека» [7, с. 142].

В умовах глобалізації та взаємозалежності держав соціальна безпека набуває нового значення. Відтак, ідеться не лише про внутрішню соціальну стабільність, а й про міжнародну співпрацю та інтеграцію в глобальну систему безпеки.

Система забезпечення національної безпеки спрямована на запобігання можливим загрозам національним інтересам, а в разі їх виникнення-на їх нейтралізацію та мінімізацію наслідків. Існування загроз національним інтересам актуалізує питання зміцнення та забезпечення національної безпеки [12, с. 69].

Національна конкурентоспроможність і національна безпека є взаємопов'язаними явищами, як і поняття державна безпека та національна безпека [6, с. 65], які визначають статус, роль і перспективи держави у міжнародному співтоваристві. Для підвищення національної конкурентоспроможності та національної безпеки в майбутньому необхідно здійснити комплексне реформування та модернізацію в усіх сферах. Головним стратегічним орієнтиром [11, с. 80]. України у сфері національної безпеки є створення належного національного потенціалу як основи для забезпечення безпеки та стійкості країни.

Національна ідентичність як об'єкт національної безпеки оперує поняттями «нація», «національна безпека» та «самоідентичність» у взаємодії з поняттями «дезінформація», «кризова ситуація» [16, с. 81].

Національна інформаційна безпека має гарантувати недоторканність національних переконань та сприяти їх поширенню. Особливий інтерес становить процес формування єдності українців, що є головним чинником збереження держави [13, с. 15].

Вирішення проблем державного будівництва, створення ефективних механізмів соціального захисту населення та стабілізації політичного процесу неможливе без розробки комплексної державної політики у сфері національної безпеки та забезпечення її реалізації в Україні [4, с. 18]. Складна політична та економічна ситуація в державі, зростання загроз інтересам громадян, суспільства і держави зумовлюють необхідність вироблення дієвих заходів щодо забезпечення національної безпеки.

Остання правозахисна ініціатива Ради Європи спрямована на регулювання прав людини в контексті розвитку інформаційних технологій [15, с. 49]. Документ «Інформаційне суспільство: у фокусі до 2021 року» [3, с. 47] визначає основні сфери захисту прав у цифровому середовищі: свобода вираження поглядів, цифрове врядування, штучний інтелект, приватність та боротьба з кіберзлочинністю; Стратегія управління Інтернетом та діяльність Спеціальної комісії з питань штучного інтелекту (САНАІ) стає наразі для України візією адаптації європейських стандартів до українського законодавства.

Необхідність внесення змін та доповнень до низки положень з урахуванням особливостей режиму воєнного стану – стратегічна потреби України. Для формування та розвитку системи національної безпеки необхідно розробити Концепцію (основи) національної безпеки України як державний документ, що відображає загальну ідею реалізації державної політики у цьому напрямі. Цей концептуальний документ має визначити національні інтереси, чинники, що загрожують національним інтересам і безпеці, та напрями діяльності із забезпечення життєво важливих національних інтересів і протидії сучасним загрозам і викликам [14, с. 281].

Отже, навіть пропри значну кількість наукових розвідко із указаної тематики, усе ж невирішеними залишаються візійні питання національної безпеки в умовах інфосуспільства.

Метою дослідження визначаємо аналіз впливів інформаційного суспільства на національну безпеку, а також надання рекомендацій щодо роботи з базовими загрозами в контексті безпеки інформації і шляхів їх нейтралізації.

Завдання. У ході опрацювання цієї мети ставимо перед собою такі завдання:

- дати характеристику сутності і специфіці інформаційного суспільства;
- провести дослідження основних викликів

і загроз в контексті інформаційної безпеки;

- опрацювати світовий досвід та практики впровадження інформаційної безпеки;

- надати рекомендації зміцнення нацбезпеки в контексті інформаційного суспільства

Методи дослідження: для якісного вирішення поставлених завдань за методологічну основу окреслюємо системний аналіз (в контексті порівняння впливів інформаційного суспільства та нацбезпеки); компаративний аналіз (в контексті дослідження міжнародного досвіду у сфері); контент-аналіз з метою оцінки впливу інформаційної війни та дезінформаційних технологій, а також прогностику з метою визначення перспективних візій розвитку інформаційної безпеки в Україні на етапі війни**.**

Виклад основного матеріалу. Безпека держав, соціальна динаміка та економічний розвиток – це ті стратегічні ресурси, на які в сучасному світі інформація впливає найбільше. Створення нових можливостей для прогресу і нових викликів зумовлене розвитком цифрових технологій, глобальної взаємодії, мережевої комунікації, відтак є переходом до інформаційного суспільства. Наразі нацбезпека використовує значну кількість цифрових технологій, однак рівень цього використання спонукає підвищувати здатність держави захищати власний інформаційний простір від зовнішніх і внутрішніх посягань. Штучний інтелект у сфері аналізу, розвиток глобалізації, Інтернету, популяризація медіа несуть загрозу ризиків дезінформації, кібератак та маніпуляції свідомістю суспільства, відтак особливо актуальною є потреба забезпечувати інформаційну безпеку як невід'ємний компонент безпеки держави. Таке розуміння охоплює розвиток інфраструктури, кібербезпеки, захист інформаційних ресурсів, зупинка пропаганди і деструктивних інформаційних впливів, гібридні загрози, які містять елементи інформаційного, військового, політичного, економічного впливу та відображається на національній безпеці, а робота проти них потребує комплексного підходу.

Наразі Україна піддається неперервним атакам кібератресії в контексті повномасштабного вторгнення та намагається знайти вихід із ситуації спротиву. Традиційні механізми регулювання такого спротиву на державницькому рівні потребують перегляду, позаяк вони не відповідні до викликів цифрової епохи.

Із метою опрацювання окресленої проблематики необхідно розпочати з теоретико-методологічних засад національної безпеки в інформаційному суспільстві, а також розуміти, що поняття інформаційне суспільство має певні особливості.

Почнемо з дефініції. Інформаційне суспільство – це такий вид соціального устрою, де головними факторами розвитку суспільства є продукування, обробка та поширення інформації.

У формуванні соціальних процесів суб'єктом дії в ньому є інформація, а об'єктами дії – цифрові технології та комунікаційні точки. Динамічність суспільства піддається стрімкому розвитку технологій; правові регуляторні механізми в цьому контексті не є адаптованими. Це може ускладнити процес забезпечення нацбезпеки, позаяк загрози інформаційного простору стають усе більш розвиненими. На цій підставі необхідно розробляти адаптивні стратегії інформаційного захисту, які будуть працювати. Штучний інтелект та автоматизація роботи з інформацією сприяють наразі підвищенню ефективності процесів, але підсвічують нам нові ризики, що пов'язані з маніпулятивними впливами на свідомість громадян, використанням і поширенням персональних даних, а також шерингом фейкових новин.

Культурна, політична, кібербезпека та інфобезпека є складовими нацбезпеки в інформаційному суспільстві. Їхній узаємозв'язок забезпечує стійкість держави в межах впливу сучасних загроз та формує комплексний підхід до їхнього аналізу.

Культурна безпека пов'язана з захистом національної ідентичності і історичної пам'яті: національну єдність може підірвати використання соціальних мереж для поширення чужорідних цінностей та світоглядів. Держава повинна забезпечувати розвиток власного культурного простору і сприяти зміцненню патріотизму і суспільної згуртованості через підтримку національного інформаційного контенту. Широке застосування впливів на політичні інтереси вибори формування громадської думки – це відповідальність політичної безпеки. Дуже часто недружні сили та іноземні держави вдаються до застосування інформаційних кампаній, щоб маніпулювати політичною ситуацією; серйозною загрозою для роботи держорганів, владних структур, суспільства та бізнесу є хакерські атаки. Кібербезпека повинна здійснювати заходи з метою захисту критично важливої інформаційної структури та знищення шкідливого програмного забезпечення від несанкціонованого доступу.

Інформаційна безпека повинна боротися з дезінформацією, неправдивими новинами, втручанням у внутрішні процеси і маніпуляціями громадською думкою. Саме інформаційні війни є об'єктом дії інформаційної безпеки, яка повинна реагувати на стійкість національного медіапростору та бути здатною протидіяти спробам дестабілізації ситуації у певній державі.

На цій підставі інформаційне суспільство повинне вишукати єдиний механізм об'єднання названих складових та укладення їх у межах стратегії інформаційного захисту, що дозволить упровадити новітні технології кіберзахисту та посилювати державну політи-

ку в контексті, у тому числі медіаграмотності.

Саме такий підхід забезпечує стабільність та неперервність функціонування інформаційного простору держави у епоху цифровізації.

Вивчаючи окреслену тему, неможливо оминути питання інформаційних загроз та викликів для національної безпеки. У цьому контексті важливим є вивчення кібербезпеки та її складових: кібератак, інформаційних воєн та хакерських атак.

Кібербезпека, як показує практика, стала однією з базових складових нацбезпеки в контексті розвитку інформаційного суспільства. Державні установи, критична інфраструктура, приватні та бізнес-компанії зазнають постійних кібератак, що можуть призводити до серйозних політичних і економічних наслідків. Хакерські активісти та злочинні угруповування активно використовують кіберпростір для того, щоб збирати розвідувальні дані, саботажувати або шантажувати інструментом геополітичного впливу, який почали активно застосовувати держави. Варто пам'ятати, що є інформаційні війни, відтак вони охоплюють поширення неправдивої інформації, використання соцмереж для створення напруження в суспільстві, а також маніпуляції думкою громадян; вони активно втручаються в процеси виборчої демократії та викликають соціальні заворушення. Хакерські атаки нині є потужним елементом гібридної загрози сучасного інформаційного суспільства, прикладом є банківські атаки або ж злам систем, як це відбулося нещодавно в Україні.

Шкідливе програмне забезпечення, використання програм-вимагачів, втручання в мережу даних сторонніми особам є прикладами шкідливого програмного забезпечення та типовими методами хакерів.

Держава впроваджує спеціальні програми кіберзахисту для того, аби уникнути або зменшити вплив кібератаки на порядок і внутрішній устрій держави.

Україна зокрема активно розвиває матрицю кібербезпеки і співпрацює з міжнародними партнерами, щоб стандарти захисту інформаційного простору активно працювали та відбивалися в нормативно-правовому регулюванні.

Також необхідно пам'ятати, що фейкові новини, маніпулятивні віяння і наявність інформаційних атак дозволяє поширювати пропаганду та дезінформацію, що негативно потужно впливають на громадську думку і стратегію поведінки держави на міжнародному рівні. Вони активно поширюються в соціальних мережах та на інформаційних платформах, що дозволяє розмножувати матрицю вигідних агресорові меседжів, які можуть вплинути на політичні рішення громадян. У протилежному варіанті – вплив пропаганди і дезінформації, безумовно, наносить шкоди нацбезпеці і може мати довгострокові наслідки, у тому числі сприяти розколу суспільства, підривати довіру до демократичних інституцій та поширювати паніку.

Для забезпечення ефективної протидії названим загрозам необхідно застосовувати практику світового досвіду забезпечення інформаційної безпеки розглянемо, зокрема політику стратегії країн Європейського Союзу, Сполучених Штатів Америки, Китаю щодо інформаційної безпеки та впровадження директив комплексної стратегії і політик, наприклад, Європейський союз потужно працює над забезпеченням інформаційної безпеки у контексті реалізації комплексних стратегічних політик, наприклад, існує директива NISTU, у якій прописані жорсткі вимоги для критичної інфраструктури за основними ознаками кібербезпеки. Сполучені Штати мають стратегію кібербезпеки, яку ухвалив Білий дім; у Сполучених Штатах існує агентство кібербезпеки та безпеки інфраструктури CISA, основним завданням якого є координація захисту державних і приватних сфер від впливу кіберзагроз.

Китай має жорстоку політику контролю над інформаційним простором та розвиває власні технологічні платформи. У цьому контексті важливо, щоби держави комунікували між собою, розвивали міжнародне співробітництво та висловлювали одна одній активну підтримку в співпраці щодо розширення матриці кіберзахисту. Загалом необхідно рухатися до розуміння, що усі політики інформаційної безпеки потужних держав повинні мати спільну рису, тобто бути спрямованими на зниження кіберризиків та визначати нормативно-правове регулювання розвитку міжнародної співпраці і технологій.

Із посиленням кібербезпеки у кожній сфері на противагу цьому досі існує конкуренція між країнами щодо наявності лідерства в сфері кібербезпеки та інформаційних технологій, наприклад, Сполучені Штати і ЄС хочуть зменшити вплив Китаю на світовий кіберпростір і на цій підставі активно вводяться санкції проти it-компаній Китаю.

Ключовою міжнародною ініціативою у сфері інфобезпеки є зміст будапештської Конвенції про кіберзлочинність, яка була ратифікована багатьма державами. Саме вона описує загальні правила і принципи боротьби з кіберзлочинами і встановлює механізми міжнародної співпраці: ООН має групу урядових експертів з метою розробки правил поведінки держав у кіберпросторі та запобігання кібератакам; НАТО формує стратегію кібероборони, зокрема, у Талліні є центр передового досвіду з кібероборони, який навчає експертів в Європейському Союзі. Підтримана ініціатива протидії гібридним загрозам: у Європейському центрі протидії гібридним загрозам відбувається координація країн-членів в боротьбі з кібератаками та дезінформацією. Усім державам в цьому контексті важливо боротися з

фейковими новинами. У світових пошуковиках запроваджено спеціальний алгоритм, що здатен виявляти і блокувати дезінформацію, однак попри все значна кількість багатьох міжнародних ініціатив не врегульовує повністю питання безпеки кіберпростору, оскільки Росія наполягає на суверенному контролі над Інтернетом, що виливається у неперервні атаки на інформаційні системи інших держав, зокрема України.

На цьому зрізі штучний інтелект в інформаційній безпеці здатен аналізувати значні обсяги даних, а також відігравати важливу роль у виявленні підозрілих активностей в режимі реального часу.

Автоматизацією та виявленням загрози займаються компанії, які розробляють програмні рішення для ідентифікації кібератак до моменту завдання ними шкоди. Штучний інтелект бореться з дезінформацією та впроваджує алгоритми аналізу джерел інформації: на основі рівня їхньої надійності перспективне використання в найближчому майбутньому може отримати нейромережа, яка аналізує поведінку користувачів.

Нині Україна не має добре розвиненої законодавчої бази, яка регулює питання інформаційної безпеки. Законом України № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» визначено основні напрями політики захисту нацбезпеки. Державна служба спецзв'язку та захисту інформації в Україні несе відповідальність за кіберзахист інформації в державних структурах.

Підзаконні акти посилюють контроль над цифровими платформами та здійснюють регулювання обігу інформації під час гібридної війни, а також можуть використовуватися для аналітики поширення дезінформації.

Із 2014 року Україна потерпає від масштабних інформаційних атак українське законодавство забороняє використання та поширення російських соцмереж; діє активна боротьба проти пропаганди в цифровому просторі; неперервно запроваджується санкції щодо російських засобів масової інформації, які поширюють фейкову інформацію; посилюється контроль над інфраструктурою телекомунікації з метою недопущення атак у сфері новин.

Однак, навіть попри всі державній і волонтерські зусилля, інформаційна безпека України все ж має перелік проблем та недоліків, які провокуються недостатнім фінансуванням, відсутністю кваліфікованих спеціалістів та слабкою координацією роботи державних структур.

Захист інформації та національної безпеки ускладнює відсутність уніфікованої стратегії реагування на кіберзагрози; складно модернізувати технологічну базу за відсутності відповідного фінансування; дефіцит кваліфікованих кадрів у сфері інфобезпеки породжує відсутність кваліфікованої допомоги та оперативного реагування на щоденні виклики; державні установи не можуть самостійно виявляти і нейтралізувати загрози через відсутність ефективних ресурсів регуляції.

Проблемним залишається контроль дезінформації, однак Україна має перспективи щодо зміцнення інформаційної безпеки в контексті співпраці з НАТО і ЄС задля модернізації і посилення інформаційного простору. Серед ключових напрямків розвитку співпраці є модернізація законодавства і впровадження штучного інтелекту, а також посилення безпеки критичної інфраструктури та розвиток власної системи інфозахисту. Необхідно також підтримувати розвиток навчальних концептів для громадян та публічних службовців і стимулювати розвиток регіональних та національних it-компаній, які можуть самостійно розробляти концепцію кіберзахисту. У цьому контексті важливо залучати міжнародних партнерів для апробації новітніх технологій, їхнього бета-тестування та підвищення рівня нацбезпеки через підвищення рівня інформаційної безпеки громадян.

Висновки та перспективи подальших досліджень. Опрацювавши тематику в контексті національної безпеки інформаційного суспільства, можемо надати рекомендації, дотримання яких значною мірою покращить роботу фахівців у цій сфері та дасть бажаний і очевидний результат.

Найперше, із чого треба почати – посилювати розвиток національної системи кібербезпеки через створення уніфікованої єдиної державної платформи, яка моніторитиме та аналізуватиме систему кіберзагроз, працюючи з інтеграцією даних державних установ, міжнародних партнерів та приватного сектору. У межах створення платформи необхідно посилювати законодавчі ініціативи, які регулюватимуть обов'язкове впровадження систем кіберзахисту в критично важливій інфраструктурі та державних установах. Активізація співпраці з міжнародними організаціями дозволить обмінюватися інформацією про можливі кіберзагрози та надасть варіанти їхнього спротиву.

Друге, на що необхідно звернути увагу, - це інтегрувати штучний інтелект в систему інформаційної безпеки через впровадження технологій машиночитного навчання з метою автоматичного виявлення та нейтралізації компаній, що несуть дезінформацію. Штучний інтелект необхідно застосовувати в аналізі великих масивів даних з аналітикою і прогнозуванням потенційних кіберзагроз. Інтеграція штучного інтелекту також може стати точкою співпраці технологічних компаній та державних установ задля створення спільних напрацювань у сфері кіберзахисту.

Третій крок: посилювати медіаграмотність та протидіяти дезінформації; обов'язкові кур-

си медіаграмотності у всіх навчальних закладах усіх рівнів підвищать стійкість наймолодших громадян, громадян середнього віку, а також старших громадян, і зробить їх стійкими до маніпулятивних технологій. Державна підтримка незалежних фактчекінгових організацій повинна бути розширена задля того, щоб активно і неперервно здійснювати аудит достовірності інформації. На цій підставі необхідно встановлювати механізми швидкого реагування на завдані інформаційні атаки, у тому числі спростовувати фейкові новини в офіційних джерелах.

Усі напрацювання будуть успішними тільки в тому разі, якщо посадовці будуть виходити з ініціативами щодо вдосконалення нормативно-правової бази, відтак є необхідність гармонізувати українське законодавство з міжнародними стандартами та нормами НАТО і ЄС у частині кіберзахисту і кібербезпеки.

Нові положення законодавства повинні містити жорсткі вимоги щодо захисту персональних даних громадян, непередачі їх третім особам, а також роботи соцмереж, цифрових платформ. Законодавчі механізми повинні містити різнорівневі відповідальності для фізичних і юридичних осіб, які були зафіксовані на рівні дезінформаційних або інформаційних атак.

Фінальним кроком буде створення єдиної державної екосистеми кібербезпеки, яка, на наше переконання, буде підтримувати стартапи у сфері штучного інтелекту та кібербезпеки і розвиватиме різнорівневу співпрацю громадянського суспільства, бізнесу і державного сектору. Для комплексного підходу у вивченні новел інформаційної безпеки національна екосистема кібербезпеки допоможе запровадити системи сертифікації для всіх компаній, які прямо або опосередковано надають послуги у сфері інфотехнологій.

Резюмуємо, що невід'ємною частиною нацбезпеки є інформаційна безпека, а її вивчення, забезпечення і імплементація вимагають комплексного аналізу та підходу до впровадження.

Провідні країни світу активізують важливість стратегічного планування, технологічного розвитку та міждержавної співпраці у сфері кібербезпеки. Значні інформаційні загрози, із якими стикається Україна з 2014 року, активізують різнорівневу адаптацію механізмів захисту, однак досі залишається гострою потреба гармонізації нормативно-правових актів у сфері кібербезпеки та підвищення рівня підготовки спеціалістів із імплементації технологій нацбезпеки в інформаційне суспільство.

Перспективою подальших досліджень вбачаємо інтеграції штучного інтелекту з метою прогнозування атак, розвиток базових національних систем моніторингу для посилення інформаційного впливу на міжнародному рівні. Безумовно, важливо аналізувати психологічні аспекти нацбезпеки в інформаційному суспільстві та вплив соціальних мереж, а також дестабілізаційні візії і методи протидії гібридним загрозам в інформаційному суспільстві. Кращі міжнародні практики та їх поширення дозволять адаптувати методологію до українських реалій.

У довгостроковій перспективі вбачаємо розробку національної екосистеми кібербезпеки з метою утвердження сталого захисту українського інформаційного простору та нацбезпеки в інформаційному суспільстві.

Список використаних джерел

1. Балацько Л. (2009). Національна безпека України: загрози та виклики. «Дипкорпус» суспільно-політичний часопис. URL: http://dipcorpus-info.at.ua/news/2009-04-21-1.
2. Баліцький В. (2024). Гносеологія формування понять «Безпека», «Державна безпека» та «Національна безпека». Litopys Volyni. 183-188. https://doi.org/10.32782/2305-9389/2023.29.29.
3. Бочарова Н., Шкабаро В., Палєєва Ю. (2021). Принципи і пріоритети Ради Європи щодо захисту прав людини в інформаційному суспільстві: ініціативи. Інформаційне суспільство: Фокус 2021. Актуальні проблеми держави і права. 45-50. https://doi.org/10.32837/apdp.v0i90.3206.
4. Воронкова А., Храпач К. (2024). Національна безпека в умовах мінливого середовища: запобігання загрозам та викликам. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 16-22. https://doi.org/10.32689/2523-4625-2023-6(72)-3.
5. Дикий А., Наумчук К., Тростенюк Т. (2021). Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір. Вип. 176. С. 155-158. https://doi.org/10.32782/2224-6282/176-28.
6. Кобко Є. (2022). До проблеми визначення поняття «Національна безпека». Вісник Пенітенціарної асоціації України. 62-70. https://doi.org/10.34015/2523-4552.2022.1.07.
7. Куц Г. (2020). Концептуалізація понять «Національна безпека» і «Державна безпека» у політико-правовому дискурсі. Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки. 1. 139-153. https://doi.org/10.34142/24130060.2020.20.1.13.
8. Кучменко В., Тишкул Я. (2024). Оцінка сучасного стану національної безпеки України. Таврійський науковий вісник. Серія: Публічне управління та адміністрування. 41-50. https://doi.org/10.32782/tnv-pub.2024.4.4.
9. Павленко В. (2022). Щодо визначення поняття «Безпека держави»: проблеми теорії та практики у сучасних умовах України. New Ukrainian Law. 103-110. https://doi.org/10.51989/NUL.2022.3.15.
10. Резнікова О. (2022). Стратегічний аналіз безпекового середовища України. Стратегічна панорама спеціальний випуск. С. 45-53. URL: https://www.researchgate.net/publication/365432129_STRATEGIC_ANALYSIS_OF_UKRAINE%27S_SECURITY_ENVIRONMENT.

11. Ситник Г., Таран Є. (2024). Концептуальне осмислення взаємозалежності феноменів «Конкурентоспроможність держави» та «Національна безпека». Herald of Khmelnytskyi National University. Economic sciences. 326. 77-81. https://doi.org/10.31891/2307-5740-2024-326-13.
12. Турченко О., Груценко Ю. (2023). Національна безпека і державна безпека: поліваріантність визначення та співвідношення. Правничий часопис Донецького національного університету імені Василя Стуса. 66-74.https://doi.org/10.31558/2786-5835.2023.2.8.
13. Fedorchuk V. (2023). National consciousness in the field of information security of society. European Humanities Studies: State and Society. 4-18. https://doi.org/10.38014/ehs-ss.2023.4.01.
14. Hubarieva I., Khaustova V., Trushkina N. (2024). Нормативно-правове та організаційне забезпечення національної безпеки в Україні / The Regulatory and Organizational Support of National Security in Ukraine. Business Inform. 11. 277-293. https://doi.org/10.32983/2222-4459-2024-11-277-293.
15. Kurylo V., Karaman O. (2024). The security of civil society and its role in ensuring national security in the conditions of the Russian Federation's war against Ukraine. Social pedagogy: theory and practice. 44-54. https://doi.org/10.12958/1817-3764-2024-3-44-54.
16. Lemak O. (2025). National consciousness as the most priority object of ensuring national security. Uzhhorod National University Herald. Series: Law. 1. 78-89. https://doi.org/10.24144/2307-3322.2024.86.1.11.

References

1. Balatsko L. (2009). Natsionalna bezpeka Ukrainy: zahrozy ta vyklyky (National security of Ukraine: threats and challenges). "Dipkorpus" suspilno-politychnyi chasopys. URL: http://dipcorpus-info.at.ua/news/2009-04-21-1.
2. Balitskyi V. (2024). Hnoseolohiia formuvannia poniat "Bezpeka", "Derzhavna bezpeka" ta "Natsionalna bezpeka" (Gnoseology of the formation of the concepts "Security", "State Security", and "National Security"). Litopys Volyni. 183-188. https://doi.org/10.32782/2305-9389/2023.29.29.
3. Bocharova N., Shkabaro V., Paliieva Y. (2021). Principles and priorities of the Council of Europe regarding human rights protection in the information society: initiatives. Information Society: Focus 2021. Actual Problems of State and Law. 45-50. https://doi.org/10.32837/apdp.v0i90.3206.
4. Voronkova A., Khrapach K. (2024). National security in a changing environment: preventing threats and challenges. Scientific Works of the Interregional Academy of Personnel Management. Political Science and Public Administration. 16-22. https://doi.org/10.32689/2523-4625-2023-6(72)-3.
5. Dykhyi A., Naumchuk K., Trosteniuk T. (2021). Analysis of modern threats to state information security. Economic Space. 176. 155-158. https://doi.org/10.32782/2224-6282/176-28.
6. Kobko Ye. (2022). On the problem of defining the concept of "National Security". Bulletin of the Penitentiary Association of Ukraine. 62-70. https://doi.org/10.34015/2523-4552.2022.1.07.
7. Kuchmenko V., Tyshkul Ya. (2024). Assessment of the current state of Ukraine's national security. Tavriiskyi Scientific Bulletin. Public Administration Series.41-50.https://doi.org/10.32782/tnv-pub.2024.4.4.
8. Kuts H. (2020). Conceptualization of the concepts "National Security" and "State Security" in political and legal discourse. Modern Society: Political Science, Sociology, Cultural Studies. 1. 139-153. https://doi.org/10.34142/24130060.2020.20.1.13.
9. Pavlenko V. (2022). On the definition of the concept of "State Security": theoretical and practical problems in modern Ukraine. New Ukrainian Law. 103-110. https://doi.org/10.51989/NUL.2022.3.15.
10. Reznikova O. (2022). Strategic analysis of Ukraine's security environment. Strategic Panorama Special Issue. 45-53. URL: https://www.researchgate.net/publication/365432129.
11. Sitnyk H., Taran Y. (2024). Conceptualizing the interdependence of the phenomena of "State Competitiveness" and "National Security". Herald of Khmelnytskyi National University. Economic Sciences. 326. 77-81.https://doi.org/10.31891/2307-5740-2024-326-13.
12. Turchenko O., Hrutcenko Yu. (2023). National security and state security: multivariate definition and correlation. Law Journal of Donetsk National University named after Vasyl Stus. 66-74. https://doi.org/10.31558/2786-5835.2023.2.8.
13. Fedorchuk V. (2023). National consciousness in the field of information security of society. European Humanities Studies: State and Society. 4-18. https://doi.org/10.38014/ehs-ss.2023.4.01.
14. Hubarieva I., Khaustova V., Trushkina N. (2024). The Regulatory and Organizational Support of National Security in Ukraine. Business Inform. 11. 277-293. https://doi.org/10.32983/2222-4459-2024-11-277-293.
15. Kurylo V., Karaman O. (2024). The security of civil society and its role in ensuring national security in the conditions of the Russian Federation's war against Ukraine. Social Pedagogy: Theory and Practice. 44-54. https://doi.org/10.12958/1817-3764-2024-3-44-54.
16. Lemak O. (2025). National consciousness as the most priority object of ensuring national security. Uzhhorod National University Herald. Series: Law. 1. 78-89. https://doi.org/10.24144/2307-3322.2024.86.1.11.