



ISSUE  
N°18



EUROPEAN OPEN  
SCIENCE SPACE

COLLECTION OF SCIENTIFIC PAPERS



1st INTERNATIONAL  
SCIENTIFIC  
AND PRACTICAL  
CONFERENCE

SCIENTIFIC INNOVATION:  
THEORETICAL INSIGHTS  
AND PRACTICAL IMPACTS

JANUARY 13-15, 2025, NAPLES, ITALY





**EUROPEAN OPEN  
SCIENCE SPACE**

---

**Proceedings of the 1st International Scientific  
and Practical Conference**

**"Scientific Innovation: Theoretical Insights and  
Practical Impacts"**

**January 13-15, 2025**

**Naples, Italy**

**Collection of Scientific Papers**

**Italy, 2024**

UDC 01.1

Collection of Scientific Papers with the Proceedings of the 1st International Scientific and Practical Conference «Scientific Innovation: Theoretical Insights and Practical Impacts» (January 13-15, 2025. Naples, Italy). European Open Science Space, 2025. 255 p.

ISBN 979-8-89704-952-3 (series)  
DOI 10.70286/EOSS-13.01.2025



The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.



The conference is registered in the database of scientific and technical events of UkrISTEI to be held on the territory of Ukraine (Certificate №13 dated 6.01.2025).



The materials of the conference are publicly available under the terms of the CC BY-NC 4.0 International license.

The materials of the collection are presented in the author's edition and printed in the original language. The authors of the published materials bear full responsibility for the authenticity of the given facts, proper names, geographical names, quotations, economic and statistical data, industry terminology, and other information.

ISBN 979-8-89704-952-3 (series)

***Komleva N.***

CURRENT STATE OF INTELLIGENT DIAGNOSTIC AND  
DECISION-MAKING SYSTEM DEVELOPMENT..... 96

***Страшненко Г.***

ОЦІНКА ЯКОСТІ МЕДИЧНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ  
«GLAUCOMA V1.0»..... 101

***Решетнік В., Клішов М.***

РОЗРОБКА ТА АНАЛІЗ СИСТЕМИ ОПТИМАЛЬНОГО  
ПАКУВАННЯ ОБ'ЄКТІВ У ДВОВИМІРНІЙ ПРЯМОКУТНІЙ  
КОНТЕЙНЕРІ З РЕАЛІЗАЦІЄЮ У БРАУЗЕРНОМУ ЗАСТОСУНКУ... 103

***Plitin D., Oleksiuk N.***

INFORMATION SECURITY OF THE INDIVIDUAL AS THE BASIS  
OF INFORMATION SECURITY OF THE COUNTRY..... 105

**Section: Jurisprudence**

***Руденко Н.Ю.***

ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ПРОБАЦІЙНОЇ ДІЯЛЬНОСТІ..... 109

***Подлубна Н.С., Панченко В.В.***

КОЛІЗІЙНЕ ВИРІШЕННЯ ПИТАНЬ МІЖ ПОДРУЖЖЯМ В  
КОНТЕКСТІ МІЖНАРОДНОГО ПРИВАТНОГО ПРАВА..... 111

**Section: Logistics and Transport**

***Лебідь Є.М., Старушко О.Ю., Кисса В.О., Штурмак В.О.***

ОРГАНІЗАЦІЯ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРИ ІМПОРТІ  
БУДІВЕЛЬНИХ МАТЕРІАЛІВ..... 116

**Section: Management, Public Administration and Administration**

***Метеленко Н., Попова А., Оглобліна В., Афонов Р.***

ФОРМУВАННЯ ЕКОЛОГІЧНОЇ ПОЛІТИКИ УКРАЇНИ В  
КОНТЕКСТІ ЦІЛЕЙ СТАЛОГО РОЗВИТКУ В УМОВАХ ВІЙНИ ТА  
ПОВОЄННОГО ВІДНОВЛЕННЯ..... 119

***Yashchuk T.***

SELF-MANAGEMENT AS AN EFFECTIVE WAY TO ACHIEVE THE  
STRATEGIC GOALS OF THE ORGANIZATION..... 124

---

# **INFORMATION SECURITY OF THE INDIVIDUAL AS THE BASIS OF INFORMATION SECURITY OF THE COUNTRY**

**Plitin Dmytro**

Postgraduate student

**Oleksiuk Nataliya**

Doctor of pedagogical sciences, Professor

Department of social work and management of socio-cultural activities

Ternopil Volodymyr Hnatiuk National Pedagogical University, Ukraine

In today's world, personal information security is becoming one of the most important issues, as the spread of information technology and the growth of digital information increase the use of incomplete, untimely and inaccurate information; cases of illegal use of information technology; negative information influence; unauthorized dissemination and use of information, violation of its integrity, confidentiality and accessibility [4]. Information security of a person is characterized as a state of protection of a person from influences that can change mental states and psychological characteristics, modify his or her behavior and restrict freedom of choice against his or her will and desire. It is important to understand that personal information security is not limited to technical aspects, but also has significant social components [6].

Communication in the online environment, the use of social networks, and involvement in joint projects – all this creates new opportunities for personal development, but at the same time conceals threats, as it becomes a problem for both individual users and society as a whole. The information space of a new society often becomes a tool for shaping the feelings, consciousness, and behavior of its citizens [2]. For several decades now, the world's leading countries have been developing tactics and strategies for conducting information wars, the concepts of which include the creation of means of dangerous influence on the information spheres of other countries, disruption of the normal functioning of information and telecommunication systems, and gaining unauthorized access to information resources [1]. A particular danger is posed by the unlawful use of special means of influence on individual, group and public consciousness, which causes devaluation of spiritual values and propaganda of mass culture based on the cult of violence, on newly created values that contradict spiritual and moral values traditionally accepted in society. The decline in the spiritual, moral and creative potential of the population significantly complicates the training of labor resources for the introduction and use of the latest technologies. All this refers to external sources of information security. One of the internal sources of the threat is the decline in the effectiveness of the education and upbringing system [3].

In view of this, the problems of theoretical understanding of information security, analysis and assessment of the main information threats in the context of the



Russian-Ukrainian war and practical implementation of information resistance to protect the national sovereignty and territorial integrity of Ukraine, as well as protection of the population from psychological influences and manipulations, have become particularly relevant for our country [5]. Understanding the social aspects of information security is important for developing effective strategies to protect individuals from the destructive effects of information flows and to form their information culture and literacy (the ability of a person to use modern information technologies in everyday life and professional activities; the ability to perceive and critically evaluate information, control and distribute information flows, determine the reliability of information sources, identify biased messages, unclear or ambiguous arguments, logical) [2].

The issue of information security and culture in times of war is a matter of survival for individuals, society and the state. After all, ensuring information security is not only in the interests of the state, but also in the interests of the individual in the context of ensuring his or her rights and freedoms. The basis of modern information security is data integrity, information availability, confidentiality and reliability. Information security includes not only the regulatory and political component, but also the institutional sphere, which involves the activities of the bodies that ensure it, as well as the use of software and hardware [7].

It is worth noting that in an environment where a whole range of information is designed to manipulate public opinion and human consciousness and is presented using physiological and psychological methods and means of perception, the issue of a low level of information culture is becoming increasingly important, which leads to a decrease in a person's ability to critically perceive, analyze and evaluate the information received. In this case, the ability to form one's own opinion is practically absent [5].

Today, the term «emotional fake» is actively used when emotionally colored words are used to disseminate information that affects the human psyche and allows it to be manipulated. In general, it is always necessary to critically assess information, especially in the following cases: when the source of the information is unknown, the headline is clearly manipulative, the content contains value judgments and is emotionally colored, and there is no reference to an official source of information. The tendency to manipulate is a dangerous factor in a war, which is undoubtedly being waged in full on the information plane as well. The terms «information warfare», «information weapons» and «information terrorism» have long been used, but in wartime they take on a completely different meaning in view of the threats that exist [4].

Therefore, the state's priority task is to promote the formation of an information culture in society. One of the elements of such a culture is the ability to analyze information and filter the sources of its dissemination. It is quite reasonable to believe that information security implies: an appropriate level of information culture, i.e. theoretical and practical training of an individual, which ensures the protection and realization of her vital interests and harmonious development in the information society regardless of the presence of information threats; the ability of the state to

create conditions for harmonious development and satisfaction of the individual's needs for information regardless of the presence of information threats; guaranteeing, developing and using the information environment [7]. In this context, it is necessary to note the importance of the educational component, which consists in systematic training in information security and information culture in secondary and higher education institutions, as well as advanced training for employees of state authorities and local self-government bodies who work with information [1].

It is undeniable that modern threats to information security pose a challenge far beyond the borders of the state and encroach not only on the national space but also have severe global consequences. Therefore, in order to prevent and counter modern information threats, it is necessary not only to adopt a regulatory framework but also to ensure the functioning of an institutional mechanism for ensuring information security, including the educational component [3]. It is about consistent systematic activities of state and legal institutions that would effectively implement national interests in the information sphere, would be able not only to respond in a timely manner to the spread of fake news and false information, but would also be able to prevent information conflicts and shape the information culture of society as a whole.

In addition, given the existing global threats and challenges, it seems possible to effectively counteract information aggression by involving international organizations, institutions and the international community in this process. After all, as the realities of today show, there are no borders when waging war in the information field [6].

Thus, ensuring information security in wartime is a complex technical, political and legal activity of authorized bodies aimed at protecting the state, society and human beings. In wartime, the protection of the state's information security is a priority, as it directly affects the security of society as a whole and each individual in particular.

In the future, we consider it necessary to study the mechanisms for ensuring the information security of the individual and analyze foreign experience in addressing the problem of information security of citizens.

## References

1. Золотар, О. О. (2018). Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк». 446 с. URL: [https://pdf.lib.vntu.edu.ua/books/2021/Zolotar\\_2018\\_446.pdf](https://pdf.lib.vntu.edu.ua/books/2021/Zolotar_2018_446.pdf)
2. Литвиненко, О. (2016). Інформаційна складова у сучасній гібридній війні проти України: виклики й загрози. // Українознавчий альманах. Вип. 19. С. 171–174. URL: [http://nbuv.gov.ua/UJRN/Ukralm\\_2016\\_19\\_42](http://nbuv.gov.ua/UJRN/Ukralm_2016_19_42)
3. Онищенко, С. В., Глушко, А. Д. (2022). Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз // Економіка і регіон. № 1 (84). С. 13–20. URL: <https://reposit.nupp.edu.ua/handle/PoltNTU/11315>
4. Плітін, Д., Олексюк, Н. (2024). Інформаційна культура особистості як основа її інформаційної безпеки // The I International Scientific and Practical Conference «Current methods of improving outdated technologies and methods»,

---

January 08-10, Bilbao, Spain. Pp. 412–415. URL: <http://dspace.tnpu.edu.ua/handle/123456789/31702>.

5. Плітін, Д., Ординович, В. (2024). Використання інформаційних технологій у соціальній роботі з вразливими категоріями осіб/сімей. Ввічливість. *Humanitas*, 5, 139–145. doi: <https://doi.org/10.32782/humanitas/2024.5.20>

6. Шемчук, В. В. (2020). Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*. 2020. № 1(7). С. 285–296. URL: [https://doi.org/10.32689/2617-9660-2020-1\(7\)-285-296](https://doi.org/10.32689/2617-9660-2020-1(7)-285-296)

7. Яровенко Г. М. (2018). Системний підхід до формалізації поняття «Інформаційна безпека». *Причорноморські економічні студії (Index Copernicus та ін.)*. № 34. С. 239–244. URL: [http://bses.in.ua/journals/2018/34\\_2018/52.pdf](http://bses.in.ua/journals/2018/34_2018/52.pdf)