Formation of High School Students’ Resistance to Destructive Information Influences

Mariia Astafieva[1], Dmytro Bodnenko[1], Oksana Lytvyn[1], Volodymyr Proshkin[1], and Pavlo Skladannyi[1]

[1]*Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

Today, information attacks occupy a prominent place in hybrid wars and their influence and significance are not inferior to armed aggression. Furthermore, information warfare begins long before the invading tanks and launching missiles. It continues during the so-called “hot” war, taking on more and more “sophisticated” forms, using a wide range of tools, and improving the distribution network. One of the primary targets of information attacks is civil society, which, being misinformed, disoriented, and processed by enemy propaganda, becomes an enemy ally in the “hot” phase of the war. Therefore, strengthening society’s resilience to information threats is an urgent issue for global security. This article analyzes the experience of European countries, in particular, Eastern Europe and the Baltic States, which shows that citizens’ immunity to disinformation and hostile propaganda can be strengthened through: their media and information education; development of critical thinking; and civic education. As a result of theoretical analysis of scientific sources and the results of a questionnaire survey of Borys Grinchenko Kyiv University students, the course “Counter-manipulation Strategies in Information Security” was substantiated and developed to build university students’ resistance to destructive information influences.

Keywords

Information threats, information-psychological influences, disinformation, manipulation, indoctrination, resilience, media education, information education, critical thinking.

1. Introduction

In modern society, information significantly impacts all social spheres and processes, whereby this impact can be both constructive and destructive.

Destructive information influence is carried out through strategies aimed at satisfying selfish or aggressive interests, including geopolitical ones, and threatens security in general. Such strategies use information as a weapon to weaken and demoralize the enemy.

Thanks to modern digital technologies and cross-border media, the destructive effect of these weapons is unlimited [1].

Increased attention to these threats around the world has been caused in recent years by Russia’s aggressive expansionist behavior on the world stage, which threatens the sustainable world order and global security.

To implement its imperialist plans, Russia is actively using avalanches of disinformation and destructive propaganda, which are flowing in a wide stream due, in particular, to the development of digital technologies and access to various sources of information.

EU countries are constantly working to create effective mechanisms to counteract the spread of destructive narratives of foreign propaganda. For example, to counter Russia’s disinformation campaign in 2015—an Operational Working Group on Strategic Communications of the European Union was established in the EU—East StratCom Task Force [2]; in April 2016, the European Commission adopted “Joint Framework on countering hybrid threats a European Union response” [3]; in November 2016, the European

CPITS 2023: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine

EMAIL: m.astafieva@kubg.edu.ua (M. Astafieva); d.bodnenko@kubg.edu.ua (B. Bodnenko); o.lytvyn@kubg.edu.ua (O. Lytvyn); v.proshkin@kubg.edu.ua (V. Proshkin); p.skladannyi@kubg.edu.ua (P. Skladannyi)
ORCID: 0000-0002-2198-4614 (M. Astafieva); 0000-0001-9303-6587 (B. Bodnenko); 0000-0002-5118-1003 (O. Lytvyn); 0000-0002-9785-0612 (V. Proshkin); 0000-0002-7775-6039 (P. Skladannyi)

CEUR Workshop Proceedings (CEUR-WS.org)

Parliament adopted the Resolution "EU strategic communication to counteract propaganda against it by third parties" [4]; in April 2017, a common decision was adopted by the NATO and the EU countries to create the European Centre of Excellence for Countering Hybrid Threats [5]; in December 2020, the European Commission presented "European Democracy Action Plan", which, among other things, defines measures to promote free and fair elections and counter disinformation [6].

For Ukrainian society, the ability to withstand information threats is vitally important, as Russia used information attacks on civil society in preparation for an armed attack on Ukraine and, no doubt, Russia will not stop its informational pressure even after the victory in the "hot" war, which Ukraine will surely win with the support of the entire democratic world.

The vulnerability of Ukrainians to Russian information influence is explained by the following reasons:

- Historical ties with Russia stretch back centuries; throughout this period, Russia kept using various methods (economic, cultural, informational, and military) to subjugate Ukrainian lands and Ukrainians.
- A high Russian-speaking population, a significant part of which consists of ethnic Ukrainians, deliberately Russified over the past four centuries by numerous prohibitions of the Ukrainian language and book printing, and, during the post-Soviet era, the total introduction of Russian-language education, both at school and in higher education.
- The historical amnesia of Ukrainian society, from which the historical memory was burned out (famines, mass political repression); teaching of a distorted history of Ukraine and Ukrainian-Russian relations in schools and universities.
- Religious closeness contributed to the subordination of the spiritual, religious, and church life of Ukrainians to Moscow Orthodoxy.

All these years of Russia's enslavement of Ukrainian social, cultural, and church life (in imperial Russia, in the Soviet Union, and after its collapse), Russia's complete ideological influence in Ukraine has resulted in a large part of the Ukrainian population, especially in the east and south of the country, being loyal and supportive of Russia. It allows our neighbor to declare the Russian-speaking Ukrainians Russians and to impose a toxic narrative of "one nation". Since the beginning of Russia's open aggression against Ukraine, which began in 2014 and moved into a hot phase in February 2022, the number of Russian sympathizers among Ukrainians has significantly decreased (according to the results of a survey carried out by the Kyiv International Institute of Sociology in May 2022, only 2% of respondents had a good attitude towards Russia [7]). However, none of this means these people have become resistant to Russian disinformation and propaganda.

Therefore, an urgent problem for the Ukrainian state's national security is to strengthen civil society's resilience to information threats, particularly from Russia.

2. Analysis of Previous Results

Significant changes in the geopolitical landscape and international relations in recent years, caused, in particular, by Russia's aggressive expansionist behavior on the global stage, have revealed problems in maintaining sustainable world order and security. One of the biggest threats today is the avalanche of disinformation that, thanks to technological advances, spreads in a comprehensive stream. Scientific and academic circles have actualized the concept of the resilience of states and societies to hostile information influences and malicious propaganda.

Under the term "society's *resilience* to destructive information influences", we understand the ability of citizens to recognize their sources, realize the purpose of spreading disinformation and manipulative information, and effectively counter such influences. Many studies focus on security resilience related to hybrid threats, mainly information [8, 9].

O. Filipec shared the Czech Republic's experience in strengthening society's resilience in the context of information warfare, particularly Russian disinformation and propaganda [10]. Moreover, the issue of society's resilience to global threats in different European countries is considered in the works of G. Sharkov (Bulgaria) [11], D. Smiljanic (Croatia) [12], A. Hugyik (Hungary) [13], and others.

The theoretical and methodological aspects of hybrid threats and society's counteraction to them, including using cybersecurity, are presented in the studies of J. Freedman, G. Gjørv, V. Razaka-maharav [14], the concept of "sustainability" is considered in the works of P. Fluri, T. Tagarev [15].

The latest Disinformation Resilience Index data in the Visegrad Four and Eastern Partnership countries were published in [16].

The experience of European countries, mainly Eastern Europe and the Baltic States, shows that citizens' resistance to disinformation and hostile propaganda can be strengthened through (a) their media and information education; (b) the development of critical thinking; (c) their civic education.

The purpose of the study, the results of which are presented in this article, was to identify the level of understanding of university students of the problem of individual and society's resilience to information threats and the possibility of university education to build this resilience in students during their studies.

The study resulted in the development of an interdisciplinary training course to build university students' resilience to destructive information influences [17].

3. Research Methodology

The following methods were used in the study: analysis of scientific literature to clarify the essence of information-psychological threats; analysis of online resources on this issue, methodological literature on the development of an academic discipline to form university students' resistance to destructive information influences; a survey aimed at determining the attitude of university students to the problem of society's resistance to information threats; visualization (tables, diagrams, figures) to present the results of the survey.

4.1. The Theoretical Framework of the Study

We will distinguish between two classes of information threats based on the object of influence:

- Information-technological threats, when computers and information systems became the object of influence.
- Information-psychological threats, when the object of influence is both individual and mass consciousness as well as the emotional and psychological sphere.

This article focuses on information-psychological threats and ways to build individual and social resilience to them [18, 19].

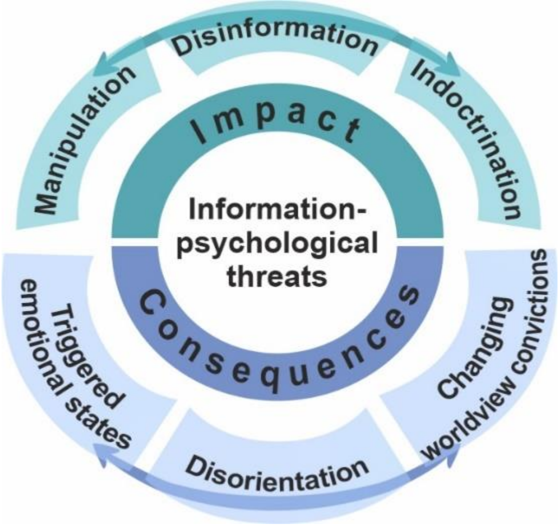
Disinformation
Indoctrination
Manipulation
Impact
Information-psychological threats
Consequences
Triggered emotional states
Disorientation
Changing worldview convictions

Figure 1: Information-psychological threats

According to the nature of the influences on the human mind, information-psychological threats will be divided into (Fig. 1):

- Threats are associated with the use of subconscious mechanisms of influence on the psyche, creating the right emotional mood, fears, anxiety, etc. (manipulation).
- Threats related to misleading people (disinformation).
- Threats associated with changing the worldview, and forming certain stereotypes (indoctrination).

Manipulation as an information threat is an act of influencing someone to create an inadequate worldview, provoking the intended emotional reaction of the target audience to make them do what the manipulator wants. For instance, before the seizure of Crimea, lies were spread about the alleged march of "Banderites" to the peninsula, which fueled separatist sentiments among the peninsula's residents.

In the following, *disinformation* will be understood as disseminating distorted, untrustworthy, or false information that leads to distortion of reality or misleading people. Disinformation can be intentional, for example, to influence public opinion, but can also be reckless when false information is disseminated due to ignorance or negligence (misinformation). An example of disinformation that discredits international military assistance to Ukraine is the Financial Times article of February 6, 2023, about alleged attempts at human and arms trafficking by Ukraine [20].

Indoctrination is imposing certain ideas, views, or doctrines by systematically influencing a person's thoughts and beliefs so that they accept these ideas as their own without substantiation or critical evaluation [21].

In our case, Russia's means of indoctrination is the deliberate distortion of Ukraine's history, destroying the self-identity of Ukrainians (for example, by positioning prominent Ukrainian scientists, artists, and religious figures as Russian, and by dominating the information space of Ukraine with Russian cultural products), incitement of inter-confessional and inter-ethnic contradictions, use of regional, ethnic, linguistic and other particular identities to form lines of division in society.

Some examples are:

- The Kremlin's narratives about the historical unity of Russians and Ukrainians, about how Lenin created Ukraine on supposedly Russian lands.
- Distribution in the media during the 2004 presidential election, allegedly from "nationalists" from the western part of Ukraine, a map dividing the country into three sorts: the Ukrainian-speaking West (Sort I), the Surzhyk-speaking Center and North (Sort II), and the Russian-speaking East and South (Sort III).

4.2. Analysis of Students' Attitudes Towards the Problems of Society's Resilience to Information Threats

In the first semester of the 2022–2023 academic year, Borys Grinchenko Kyiv University interviewed university students about their understanding of the sources of information threats to the security of the state, society, and individuals, as well as their attitude to the problem of society's resilience to information threats.

The study involved 163 students of different specialties and courses at the university.

Primarily, we wanted to find out whether students recognize that information can threaten global security (economic, industrial, social, humanitarian, etc.). The vast majority of respondents (about 94%) answered this question "yes" or "rather yes", which demonstrates the relevance of the problem of our study. Moreover, the same number of respondents (93.9%) consider the problem of information threats and the ability to counter them to be very relevant even vitally important for Ukraine today. None of the respondents thinks it is unimportant.

However, 18% of respondents claimed that they had never faced information threats, and another 44% could not recall any cases when they had been threatened by any information threat.

It indicates that many students cannot identify what exactly constitutes an information threat and have insufficient theoretical knowledge of the nature, signs, and forms of information threats. About 38% of students reported having faced information threats in their lives. However, the list of information threats mentioned by these respondents was very limited. Only a few students cited fake information related to the war in Ukraine and Russian propaganda among the examples. Other respondents in this group mentioned bullying and threats to life, information threats caused by computer viruses aimed at damaging email accounts, bank accounts, social media accounts, etc. Several participants gave examples of actions that led to information threats on the Internet: clicking on an unknown link from an unknown person, participating in a raffle from impersonation services, etc.

Altogether, it is possible to state that respondents who acknowledge the existence of information threats identified three main types of threats: violation of information confidentiality through unauthorized access, information integrity through unauthorized data modification, and restriction of access to resources with truthful information. Do students have an idea of how to counter information threats? Do they have experience covercoming information threats, preventing and countering them? It is worth noting that not all students were able to give examples of solutions to the problem they mentioned. Filtering information sources (trusting already known or official sources, ignoring suspicious sources, obtaining information from different information resources, including foreign language ones, blocking fake sources, and challenging them) was among the most common examples, and one student suggested using "common sense" to counter absurd statements of Russian propaganda.

In this context, the student's assessment of the ability of Ukrainian society and their readiness to withstand information threats is indicative (Table 1).

Table 1
Are the Ukrainian society and its members prepared to resist and counteract information threats?

Answer choices	Society (respondents' assessment), %	Students (self-assessment), %
"Yes"	14.7	37.4
"Rather yes"	62.0	57.1
"No"	3.1	0.6
"Rather no"	20.2	4.9

We can see that students highly appreciate the resilience of society to information threats (76.7% answered "yes" or "rather yes"), while their readiness to perceive and counteract such threats is even higher (94.5% answered affirmatively, with no student "admitting" that they are not ready). It should be noted that this result should not be taken as an objective indicator of the resilience of society and individuals but rather as a subjective overestimation of the relevant capacity, which is, in fact, a typical phenomenon in such surveys. For example, O. Yurkova, founder of the Ukrainian fact-checking collective Stop Fake, cites the following research results: as of 2021, 77% of Ukrainians are aware of disinformation in the media, and 62% of them are confident in their ability to identify it. However, this confidence is not confirmed by the results of the practical test (2020), which revealed only 3% of those who were able to identify false information [16].

Therefore, the analysis of students' responses revealed that a significant number of them do not know all the possible channels of information that influence them and effective ways to resist them. Thus, they do not realize that in fact, they are the object of such influence. It makes students easy targets for manipulation and malicious propaganda, despite their conviction to the contrary.

Therefore, it is quite obvious that it is necessary to prepare students for more effective work with information to develop their ability to withstand and counteract information-psychological threats.

According to students, what qualities of a person make him or her resistant to information threats? The answers received from students allowed us to unify the qualities according to three levels:

- Operational (first of all, critical and analytical thinking, which students associate with the ability to make reservations, verify information, meticulousness, attentiveness, concentration, skepticism about any information, prudence, ability to filter information, think about the situation before making a decision, ability to search for and analyze information, logic, scrupulousness, etc.).
- Theoretical (media literacy, information literacy, cybersecurity).
- Personal (emotional stability, stress resistance, ability to resist panic, determination, perseverance and full faith in the best, patience, balance, self-confidence, focus, endurance, etc.).

At the same time, it should be noted that more than a third of students (about 36%) could not name the qualities of a personality that make it possible to resist information threats.

We were also interested in students' opinions on the possibility of university training to build their resilience to information threats (Fig. 2).

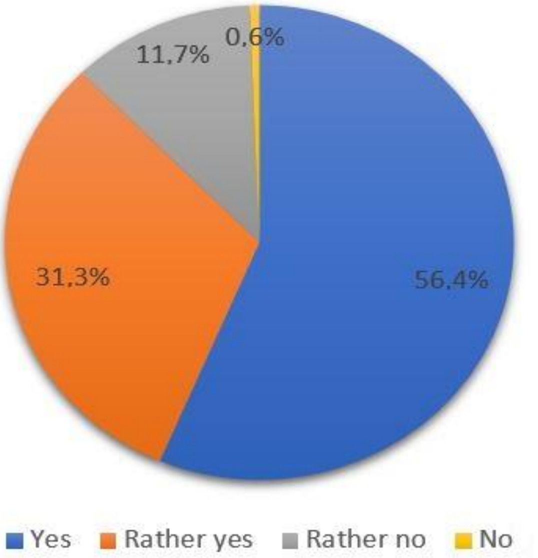

Figure 2: Students' responses to questions about the ability of university training to build resilience to information threats

According to the survey results, the vast majority of students (87.7%) believe that the university can build students' resilience to information threats, which undoubtedly opens the way for our further research. However, only half of the respondents were able to formulate their vision of such training. Here is a summary of the data. Thus, students identified the following groups of disciplines:

- Academic disciplines directly related to information literacy (computer science, cybersecurity, etc.).

- Social and humanitarian disciplines (philosophy, history, jurisprudence, introduction to the specialty).
- Psychological and pedagogical disciplines.
- Mathematical disciplines (for the development of critical thinking).

Some students noted that it is necessary as part of all academic disciplines to prepare for a resilient perception of information threats because "every discipline should teach how to analyze and filter information".

Some respondents believe that it should be a separate special ("elective") course or a series of practically oriented classes outside the curriculum.

Students consider the solution of various non-standard tasks requiring critical thinking to be effective methods of forming readiness for the sustainable perception of information threats. Among the organizational forms, students mainly mentioned the following: curatorial hours, training, master classes with the invitation of specialists who have experience in using methods and techniques of information operations, and hygiene of information use.

Thus, evaluating the results of the student survey, it should be noted:

1. Students generally believe that the problem of society's resilience to information threats is relevant for our country and global security and needs to be further addressed. They understand that information should be relevant (true at a certain point in time), reliable, reflecting reality, and objective-impartial, independent of the will and desires of a person.
2. Students' knowledge of information threats and ways to counter them is empirical, rather unsystematic, and related to individual cases in everyday life; many students are unable to identify information-psychological threats.
3. Students believe that the problem of society's resilience to information threats should be given more attention at the university, and they also recognize that university disciplines have significant potential for relevant training of students. Students also point out that it is advisable to develop and implement a special academic discipline to form their readiness for a sustainable perception of information threats and countering them.

This encourages us to develop forms and methods of preparing students to perceive information threats (the influences of inaccurate, false information, disinformation, fakes, and propaganda on the individual, society, state, etc.), and to counteract their destructive effects.

4.3. Interdisciplinary Course "Counter-Manipulation Strategies in Information Security"

The civic education of students at Ukrainian universities is provided by such disciplines as jurisprudence and, partially, the history of Ukraine, which are mandatory components of the educational programs for bachelors of all specialties. Instead, educational programs do not pay due attention to media as well as information literacy and critical thinking. That's why we offer an interdisciplinary course "Counter-manipulation Strategies in Information Security" for first-year (bachelor's) students of all specialties. The course aims to develop media and information literacy and critical thinking. Moreover, the course is also aimed at civic education, as critical thinking and media as well as information literacy are important civic competencies in the context of information warfare.

The course will be implemented in three stages (Fig. 3):

- Motivational and targeted (formation of students' awareness of the importance and significance of individual and social resilience to information threats, the ability to withstand them).
- Activity-based (development of a system of knowledge, skills, and abilities of individual protection against disinformation as well as propaganda and counteraction to these threats).
- Evaluative and reflective (analysis of the level of students' resistance to disinformation and malicious propaganda, in particular, the ability to identify these information threats, recognize their sources, realize the purpose of spreading disinformation and manipulative information and propaganda, and the ability to work more effectively with them).

The organization of educational activities is based on the principles of humanity, cooperation, and partnership between the participants of the educational process. The basis of the general methodology is a competency-based approach that involves personality-oriented, active, inquiry-based learning using digital technologies [22–24]. Implementing a research-oriented approach to teaching, tested by the co-authors of the article at Grinchenko University, has proven to be effective [25]. Students noted not only the positive dynamics of the results achieved in terms of subject knowledge and skills but also demonstrated a significant improvement in conceptual understanding and the acquisition of certain research skills: the ability to observe, analyze, doubt, ask the right questions, reflect logically, formulate a hypothesis, test it, prove facts, express opinions correctly, summarize and generalize, etc.; also recognized the effectiveness of the teaching methods used, in particular, discussion of problems, ideas, search and research in small groups.

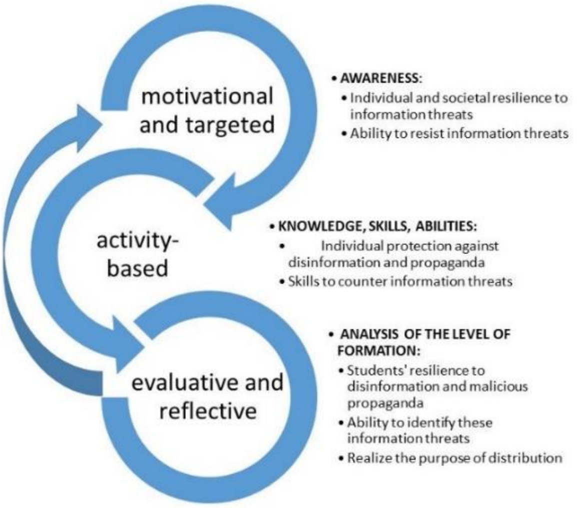
motivational and targeted
activity-based
evaluative and reflective
• AWARENESS:
• Individual and societal resilience to information threats
• Ability to resist information threats
• KNOWLEDGE, SKILLS, ABILITIES:
• Individual protection against disinformation and propaganda
• Skills to counter information threats
• ANALYSIS OF THE LEVEL OF FORMATION:
• Students' resilience to disinformation and malicious propaganda
• Ability to identify these information threats
• Realize the purpose of distribution

Figure 3: Stages in the implementation of the course "Counter-manipulation Strategies in Information Security"

Using cloud-based learning technologies motivates students to engage in project-based research learning in small groups.

Our training course is distinguished, among other things, by the fact that mathematics is chosen as a tool for developing critical thinking. The authors of the course are convinced that mathematics, like perhaps no other discipline, has inexhaustible opportunities, tools, and instruments for cultivating critical thinking. The relevant technology has been developed and tested [26].

Academic discipline "Counter-manipulation strategies in information security" consists of three content modules.

The aim of the course is:

- To form students' understanding of information threats to society, in particular, disinformation and propaganda, their sources, and ways to counteract these threats.
- To study the experience of the European Union countries in combating information threats, and tools for building civil society's resilience to disinformation and malicious propaganda.

Methods. When teaching, active methods are used (Inquiry-based learning, project-based learning, problem-based learning), a case method using cloud-based technologies. The main tool for forming critical thinking skills is mathematics.

Content Module 1: Information Literacy

Aims: to develop students' ability to solve problems of countering manipulations in the information space and to apply methods and techniques of counter-manipulations in information security.

The task is to develop students' theoretical knowledge and practical skills in the field of information security of society; skills of effective implementation of theoretical knowledge in everyday life and in working with information; and acquisition of competencies of resistance to disinformation.

Expected learning outcomes

As a result of studying the module, students should know the following:

- Content of the information warfare theory; categories, laws, patterns, and principles of information warfare.
- Information security measures.
- Forms of information warfare.
- Basic features, functions, and methods of information evaluation.
- Methods of counter-manipulation in information security.

Be able to:

- Identify signs of manipulative behavior.
- Apply methods to counteract manipulation.
- Apply methods of information evaluation.
- Apply methods and techniques of counter-manipulation in information security.

Content Module 2. Critical Thinking

Purpose: to acquaint students with the main features of critical thinking, to provide an understanding of the structure, and patterns of the logical component in the process of critical thinking, forms, and methods of argumentation, strategies, and procedures of critical thinking; to form students' awareness of the value of critical thinking.

The task is for students to acquire theoretical knowledge and practical skills, the skills of effective implementation of theoretical knowledge in everyday life and in working with information, awareness of their level of mastery of one or another method of mental activity, and motivation for further development and improvement of critical thinking.

Expected learning results

Know:

- Basics and principles of critical, rational reflection.
- Basic techniques and methods of argumentation.
- Methods and strategies of assessment and criticism.

Be able to:

- Build and recognize cause-and-effect relationships, and understand the essence of necessary, sufficient, necessary, and sufficient conditions.
- To distinguish facts from assumptions, plausible arguments from formally flawless ones, and strict proof from heuristic reasoning.
- Critically evaluate the received information, using logic and rational reasoning.
- Identify a problem, analyze it, compare, and classify.
- Conduct reasoning, and conclude, by logical laws and rules.
- To find a complete argument for assessing the situation and the correctness of the chosen way of solving the problem, taking into account the context.
- Find and correct logical errors in reasoning.
- Express yourself clearly and convincingly.

Content Module 3. Media Education

Purpose: to provide students with knowledge of European achievements in media education, media literacy, and the ability to use them to protect against misinformation and malicious propaganda for the safety of modern society.

The ***tasks*** are:

- To familiarize myself with the principles of media work in EU countries, and to learn how to analyze their media space for conscious media consumption.
- To understand how European media education influences the formation of individual consciousness in the fight against disinformation and malicious propaganda.
- To learn the leading European practices for detecting propaganda, counterfeit and manipulative media.

Expected learning results

Know:

- The main forms, methods, and means of media literacy in the EU countries to protect against misinformation and malicious propaganda.
- The role and place of media education in the European educational area.
- The key concepts and guidelines for developing media education in EU countries.

Be able to:

- Detect content from manipulative media, provide appropriate assessment, and use protective mechanisms.
- Use of modern research, selection, systematization, and reporting methods.
- Demonstrate resilience to information threats to sustain global security.

The final control is carried out as an open defense of projects. Students perform a project research task in small groups on real cases (analysis of media content, social networks, etc.).

5. Conclusions

The article theoretically reveals the phenomenon of information-psychological threats and presents the author's means of forming individual and social resistance to them.

The survey of students revealed that they consider the problem of society's resilience to information threats to be relevant for our country and global security and one that needs to be further addressed. Nevertheless, students' knowledge of information threats and ways to counter them is unsystematic.

To develop students' understanding of information threats to society, in particular, destructive information-psychological influences, their sources, and ways to counter these threats, an academic discipline "Counter-Manipulation Strategies in Information Security" has been developed that consists of three content modules: "Information literacy", "Critical thinking", "Media education". The stages of the discipline implementation are substantially disclosed:

motivational and target, activity-based, evaluative, and reflective.

Prospects for further research involve the implementation of the developed training course in the practice of university education and the evaluation of its effectiveness.

6. References

[1] H. Hulak,et al. Formation of requirements for the electronic record-book in guaranteed information systems of distance learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923, Kyiv, 2021, pp. 137–142.

[2] East StratCom Task Force, EUvsDiSiNFO.EU, 2015.

[3] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response, Eur-Lex.Europa.EU, 2016.

[4] European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda Against It by Third Parties, Eur-Lex.Europa.EU, 2016.

[5] European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE, 2017.

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On the European democracy action plan, Eur-Lex.Europa.EU, 2016.

[7] Dynamics of the Population’s Attitude to Russia and the Emotional Background Due To The War: The Results of a Telephone Survey Conducted On May 13–18, KIIS.Com.Ua, 2022.

[8] S. Bressan, A. Bergmaier, From Conflict Early Warning to Fostering Resilience? Chasing convergence in EU Foreign Policy, Democr. 28 (2021) 1357–1374. doi:10.1080/13510347.2021.1918108

[9] E. Stollenwerk, Preventing Governance Breakdown in the EU’s Southern Neighbourhood: Fostering Resilience to Strengthen Security Perceptions, Democr. 28 (2021) 1280–1301. doi:10.1080/13510347.2021.1928079

[10] O. Filipec, Towards a Disinformation Resilient Society?: The Experience of the Czech Republic, Cosmop. Civ. Soc. Interdiscip. J. 11 (2019) 1–26. doi:10.5130/ccs.v11.i1.6065

[11] G. Sharkov, Assessing the Maturity of National Cybersecurity and Resilience, Connect. Q. J. 19(4) (2020) 5–24. doi:10.11610/connections.19.4.01

[12] D. Smiljanic, Development of the Croatian National Security Strategy in the Hybrid Threats Context, Croat. Int. Relat. Rev. 23(80) (2017) 97–129. doi:10.1515/cirr-2017-0022

[13] A. Hugyik, Best Practices in the Application of the Concept of Resilience: Building Hybrid Warfare and Cybersecurity Capabilities in the Hungarian Defense Forces, Connect. Q. J. 19(4) (2020) 25–38. doi:10.11610/connections.19.4.02

[14] J. Freedman, G. Hoogensen Gjørv, V. Tahinjanahary Razakamaharavo, Identity, Stability, Hybrid Threats and Disinformation, Rev. ICONO14 Rev. Cient. Comun. Tecnol. Emerg. 19(1) (2021) 38–69. doi:10.7195/ri14.v19i1.1618

[15] P. Fluri, T. Tagarev, The Concept of Resilience: Security Implications and Implementation Challenges, Connect. Q. J. 19(3) (2020) 5–12. doi:10.11610/connections.19.3.00

[16] P. Havliček, A. Eliseev, Disinformation Resilience Index: In Central and Eastern Europe in 2021, East Center, Warsaw, 2021.

[17] V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master’s Program on Cybersecurity, in: Advances in Computer Science for Engineering and Education II, vol. 938 (2020) 610-624. doi:10.1007/978-3-030-16621-2_57

[18] R. Marusenko, V. Sokolov, V. Buriachok, Experimental Evaluation of Phishing Attack on High School Students, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 668–680. doi:10.1007/978-3-030-55506-1_59

[19] R. Marusenko, V. Sokolov, I. Bogachuk, Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation, Advances in Artificial Systems for Logistics Engineering, vol. 135 (2022)

583–594. doi:10.1007/978-3-031-04809-8_53

[20] Financial Times, Moldova’s PM calls for more EU help to curb Ukraine war smuggling, 2023.

[21] Vocabulary.Com, Indoctrination, 2023.

[22] M. Astafieva, et al., The Use of Digital Visualization Tools to Form Mathematical Competence of Students, International Conference ICTERI, 2740, Kharkiv, Ukraine, October 2020, 416–422.

[23] M. Astafieva, et al., E-learning as a Mean of Forming Students’ Mathematical Competence in a Research-Oriented Educational Process, Workshop CTE, 2643, December 2019, 674–689. doi:10.55056/cte.421

[24] D. Bodnenko, The Role of Informatization in the Change of Higher School Tasks: The Impact on the Professional Teacher Competences, International Conference ICTERI, 1000, June 2013, 281–287.

[25] M. Astafieva, et al., Experience in Implementing IBME at the Borys Grinchenko Kyiv University, Masaryk University Press, Brno 2021. doi:10.5817/CZ.MUNI.M201-9983-2021

[26] M. Astafieva, D. Bodnenko, V. Proshkin, Cloud-Oriented Training Technologies As a Means of Forming the XXI Century Skills of Future Mathematics Teachers, International Conference ICTERI, 2387, June 2019, 507–512.