"Academic Response to Hybrid Threats" Erasmus+ Capacity Building Project WARN
610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP

Evaluating Project Conferences: A Feedback Analysis (2020–2024)

Deliverable 5.3

VERSIONING AND CONTRIBUTION HISTORY

Version	Date	Revision Description	Responsible Partner
01	04/11/2024	Creation of document	SUIT (Oksana Karpenko)

This project has been funded with support from the European Commission.
This publication reflects the views only of the author,
and the Commission cannot be held responsible
for any use which may be made of the information contained therein.

Content

Introduction

State University of Infrastructure and Technologies, Kharkiv National University of Radio Electronics, HEI Academician Yuriy Bugay International Scientific and Technical University have held five Scientific and Practical Conferences "Management and Administration Responses to Hybrid Threats" (Table 1).

Table 1. Dynamics of participation in conferences "Management and Administration Responses to Hybrid Threats".

Indicators	2020	2021	2022	2023	2024
Number of participants	240	392	262	430	345
Number of scientific and higher education institutions	60	75	70	85	75
Number of countries	1 (Ukraine)	8 (Finland, France, Norway, Germany, Poland, Lithuania, Bulgaria, Ukraine)	8 (France, Norway, Germany, Poland, Italy, USA, Belgium, Ukraine)	8 (Latvia, Norway, Germany, Poland, Czech Republic, Turkey, Australia, Ukraine)	10 (Latvia, Czech Republic, Norway, Germany, Poland, Turkey, Australia, Austria, Great Britain, Ukraine)

In each conference, questionnaires have developed and offered to respondents of the plenary session.

The First All-Ukrainian Scientific and Practical Conference "Management and Administration Responses to Hybrid Threats"

2020 year's Conference was attended by 240 participants. A total of 28 respondents were interviewed (see Fig. 1).

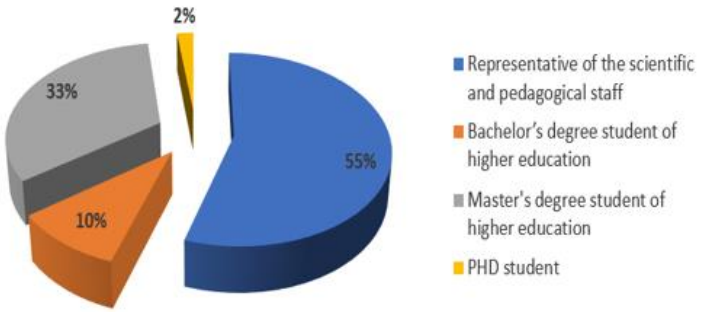

Fig. 1. The structure of survey respondents of the plenary session 2020

The results of the answer to the question "Have you ever encountered the concept of "Hybrid threats"?" are shown on Fig. 2.

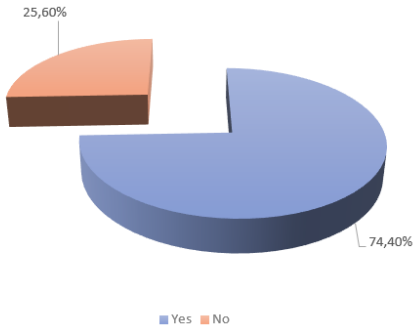

Fig. 2. The results of the answer to the question "Have you ever encountered the concept of "Hybrid threats"?"

74,4% of respondents had previously encountered such a concept. The largest number of those who have not previously encountered the concept of hybrid threats - representatives of the master's level of higher education. This result can be explained by the fact that the concept of hybrid threats is inherently complex and ambiguous, and hence the lack of clarity about its importance for respondents.

The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?" are shown on Fig. 3.

Fig. 3. The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?"

89.3% of respondents believe that countering hybrid threats is currently insufficient.

The results of the answer to the question "Do you consider it relevant to introduce into the educational process of higher education training course on combating hybrid

threats?" are shown that 89,3% of respondents gave a positive answer. This indicates the relevance of this topic and the interest in deepening knowledge and developing appropriate skills to combat hybrid threats.

The Second International Scientific and Practical Conference "Management and Administration Responses to Hybrid Threats"

2021 year's, the Conference was attended by 392 participants from 8 countries. The structure of survey respondents is shown on Fig. 4.

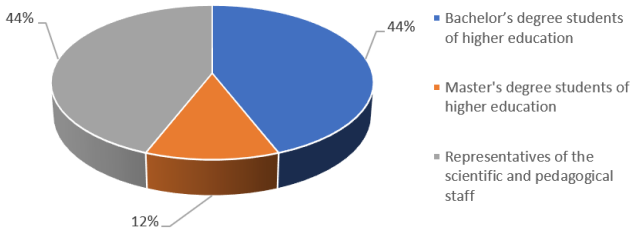

Fig. 4. The structure of survey respondents of the plenary session 2021

The results of the answer to the question "Do you consider the impact of hybrid threats on the development of the country / society / your personal life significant?" are shown on Fig. 5.

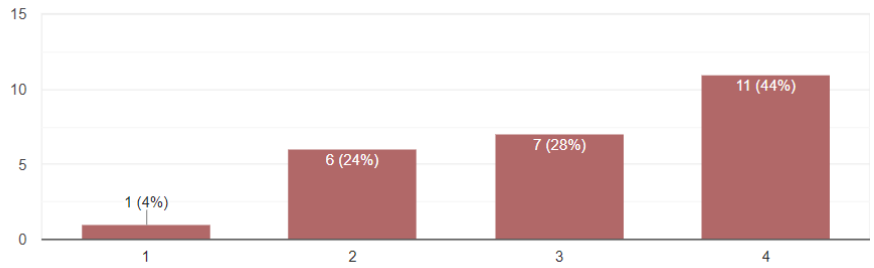

Fig. 5. The results of the answer to the question " Do you consider the impact of hybrid threats on the development of the country / society / your personal life significant?

The results of respondents' answers confirmed the significant impact of hybrid threats.

The Third International Scientific and Practical Conference "Management and Administration Responses to Hybrid Threats"

2022 year's Conference was attended by 262 participants from 8 countries. A total of 26 respondents were interviewed (see Fig. 6).

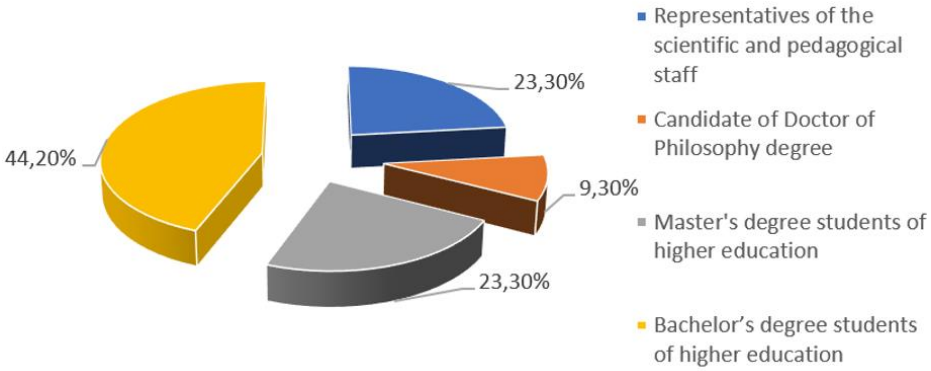

Fig. 6. The structure of survey respondents of the plenary session 2022

The results of the answer to the question "Have you ever encountered the concept of "Hybrid threats"?" are shown on Fig. 7.

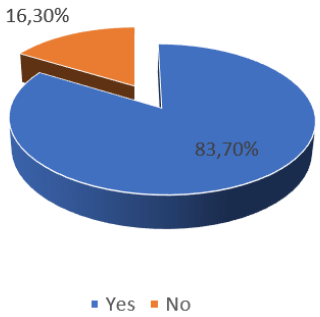

Fig. 7. The results of the answer to the question "Have you ever encountered the concept of "Hybrid threats"?"

83,7% of respondents had previously encountered such a concept. The largest number of those who have not previously encountered the concept of hybrid threats – 4 representatives of the bachelor's level of higher education and 3 representatives of the Master's level of higher education.

The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?" are shown on Fig. 8.

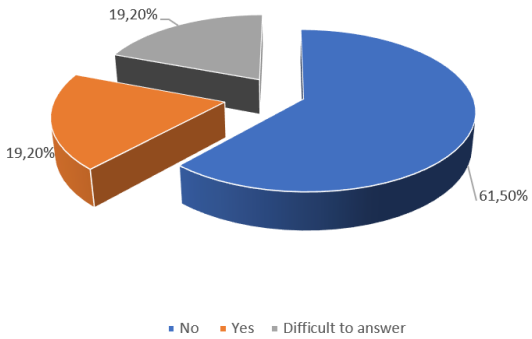

Fig. 8. The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?"

61,5% of respondents answered that currently counteraction to hybrid threats is insufficient.

The results of the answer to the question "Do you consider it relevant to introduce into the educational process of higher education training course on combating hybrid threats?" are shown that 96,2% of respondents gave a positive answer. This confirms the growing interest in increasing knowledge on this topic.

The Fouth International Scientific and Practical Conference "Management and Administration Responses to Hybrid Threats"

2023 year's Conference was attended by 430 participants from 8 countries. A total of 50 respondents were interviewed (see Fig. 9).

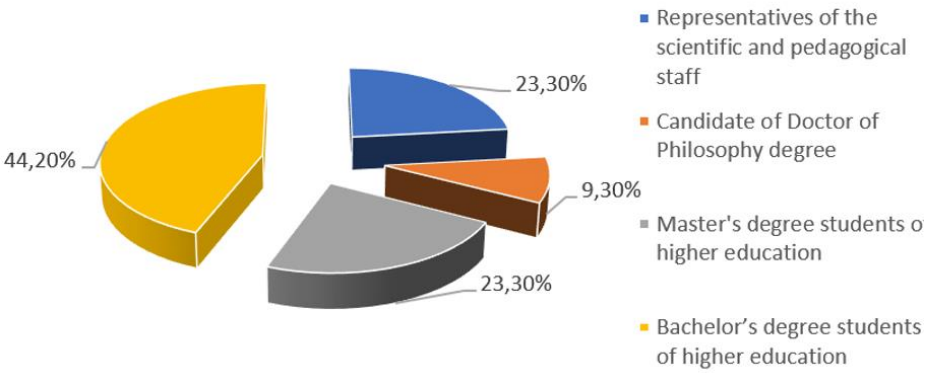

Fig. 9. The structure of survey respondents of the plenary session 2023

The results of the answer to the question "Have you ever encountered the concept of "Hybrid threats"?" are shown on Fig. 10.

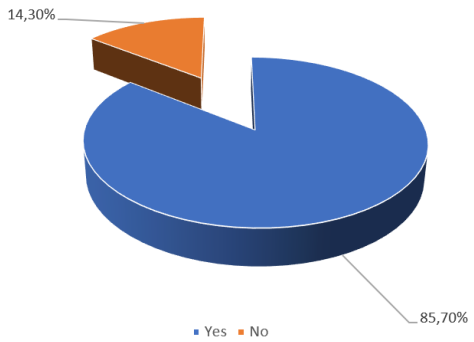

Fig. 10. The results of the answer to the question "Have you ever encountered the concept of "Hybrid threats"?"

85,7% of respondents had previously encountered such a concept. The largest number of those who have not previously encountered the concept of hybrid threats – 6 representatives of the bachelor's level of higher education, 3 Representatives of the scientific and pedagogical staff, 1 representative of the Doctor of Philosophy degree of higher education.

The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?" are shown on Fig. 11.

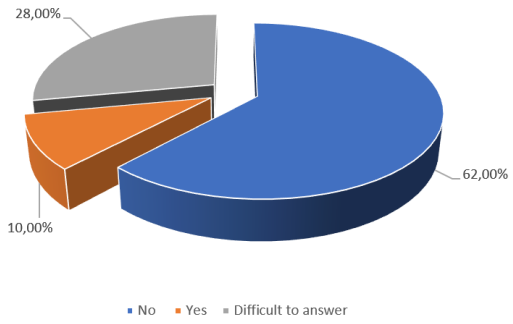

Fig. 11. The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?"

62% of respondents answered that currently counteraction to hybrid threats is insufficient.

The Fifth International Scientific and Practical Conference "Management and Administration Responses to Hybrid Threats"

2024 year's Conference was attended by 345 participants from 10 countries. A total of 100 respondents were interviewed (see Fig.12).

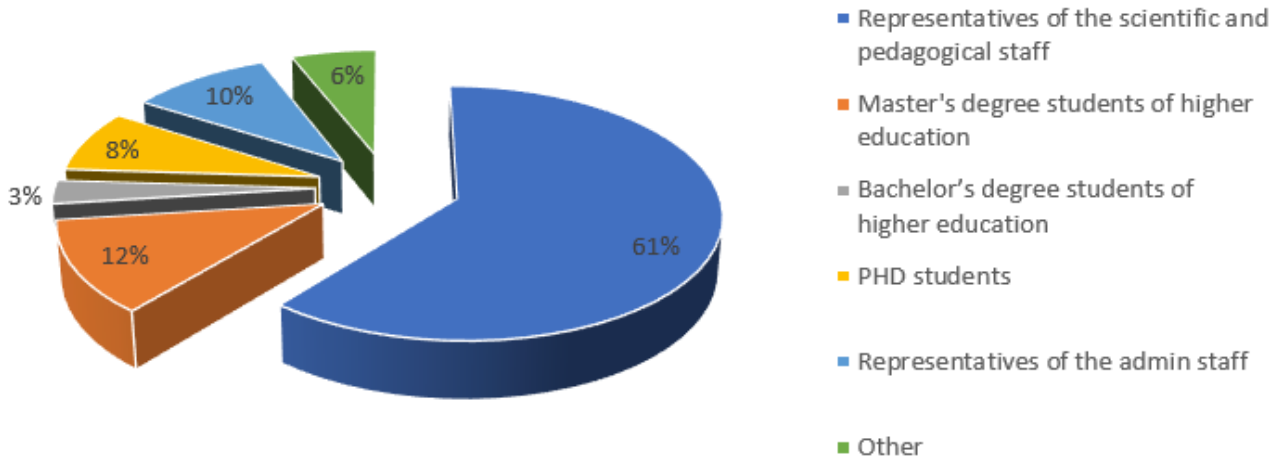

Fig. 12. The structure of survey respondents of the plenary session 2024

100% of respondents answered "Yes" to the question "Would you like to learn more about hybrid threats and measures to prevent and counter them?".

Respondents' assessments of the impact of hybrid threats on the country's development on a scale from 1 to 10 (where 1 is the least important and 10 is the most important) are shown in Fig. 13.

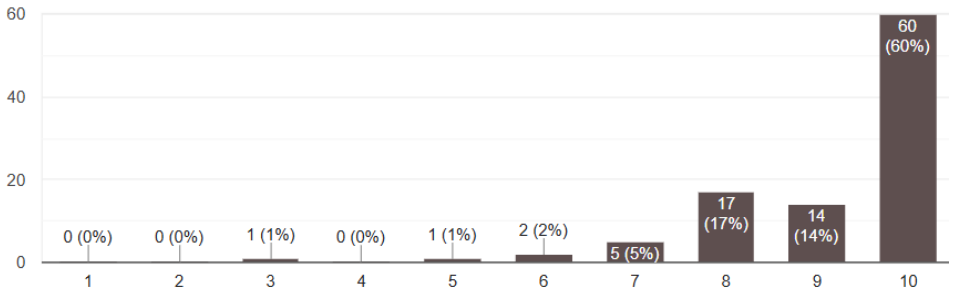

Fig. 13. Respondents' assessments of the impact of hybrid threats on the country's development

Respondents' assessments of the impact of hybrid threats on society on a scale from 1 to 10 (where 1 is the least important and 10 is the most important) are shown in Fig. 14.

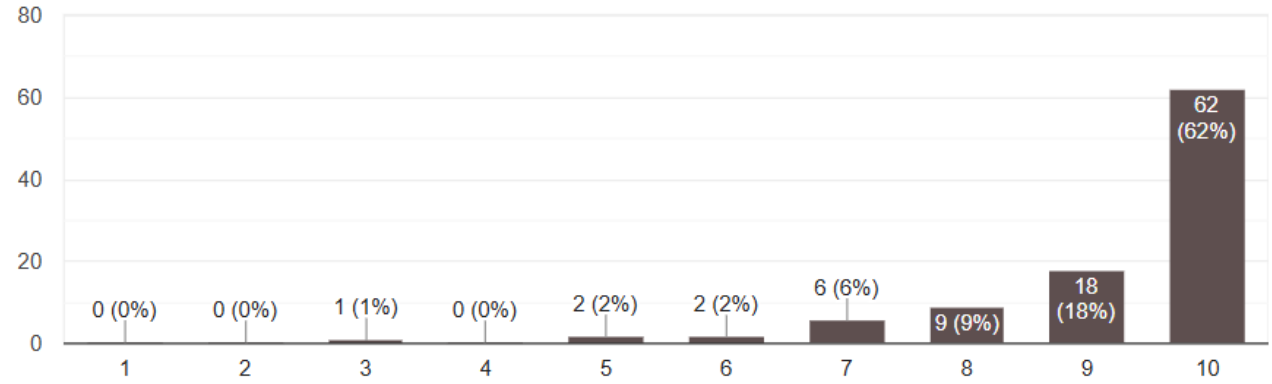

Fig. 14. Respondents' assessments of the impact of hybrid threats on society

Respondents' assessments of the impact of hybrid threats on their personal lives on a scale from 1 to 10 (where 1 is the least important and 10 is the most important) are shown in Fig. 15.

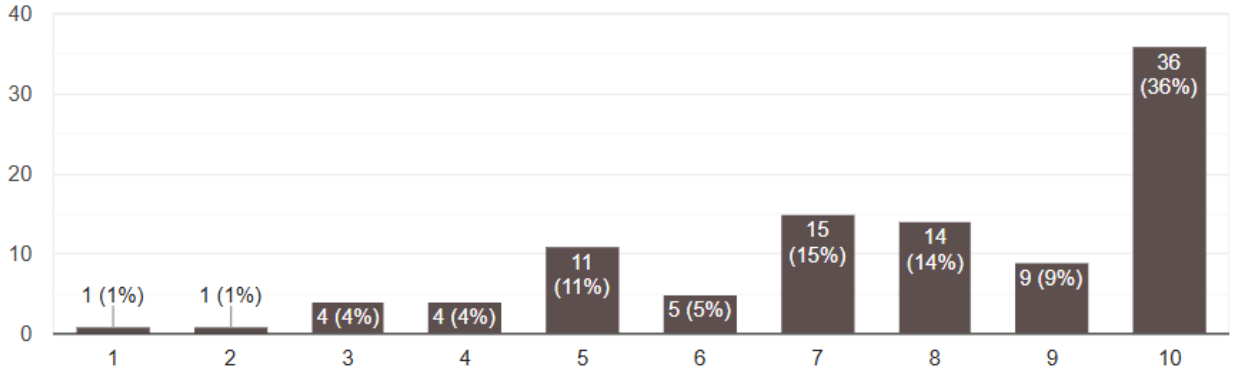

Fig. 15. Respondents' assessments of the impact of hybrid threats on their personal lives

The results of the answers to the above three questions led to the conclusion that the majority of respondents believe that hybrid threats have a significant impact on the development of the country (60 percents of respondents gave a score of “10”) and (62 percents of respondents gave a score of “10”) society. However, only 36 percent of respondents gave a score of “10” to the impact of hybrid threats on their personal

lives. This suggests that educational activities need to be continued to increase the population's resilience to hybrid threats at all levels.

The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?" are shown on Fig. 16.

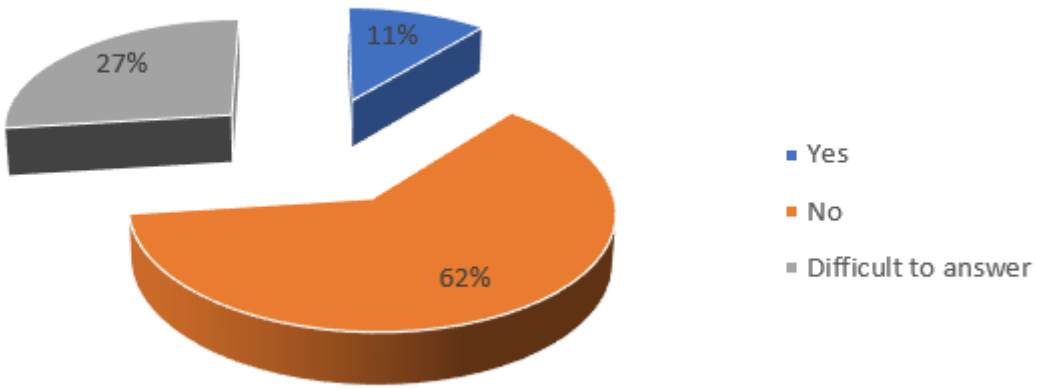

Fig. 16. The results of the answer to the question "Is it sufficient, in your opinion, to counteract hybrid threats in management in modern conditions?"

62% of respondents answered that currently counteraction to hybrid threats is insufficient. The results of the answers to this question received at all conferences confirm the need to build a Ukrainian national resilience system in order to remedy the situation at the state level.

Respondents also answered the question "Identify the industries in which, in your opinion, are currently most affected by hybrid threats?" The results are grouped as a Table 2.

Table 2 - Identify the industries in which, in your opinion, are currently most affected by hybrid threats? (the survey at the conference 2024)

Respondents	Answers
Representatives of the scientific	• education and science • education, security and defense, energy, transportation • public policy and social impact

and pedagogical staff	• military and political, education, information and communication, economy, management • information space, socio-political sphere, military sphere, economy • almost everywhere • education • economy • information space, military sphere, socio-political sphere • information sphere, cybercrime, attacks on critical infrastructure and government systems. • Military-industrial complex, Armed Forces of Ukraine, Defence Intelligence of Ukraine, Security Service of Ukraine • social and psychological perception of the population; work with segments of the population who are abroad, speak Russian, do not support national culture and teach their children this. As for the industries, I think the energy sector and the information sector • all industries are not working to their full potential • Culture, life, history of science and society • Financial sphere, energy, social sphere • Information influence on society • Education, medicine, economy • Military, intelligence, economic, political and diplomatic • Information, legal, social, political, cultural, economic and other domains of hybrid threats • Economy, industry, military, etc. • security and defense, economy, education, transportation • energy • Alerting citizens through all available resources (messengers) • agriculture • information networks, media space • education, all levels • political, economic, educational • science, education, production, government agencies • energy sector, financial and credit system, logistics, information technology • Information space • Information, culture and economy • production, industry • management, culture, politics • Media • culture, art, information • Media, culture • in the media and educational institutions • information sphere, energy, economy, finance, military • Internet • all • public administration and public communication • Education • mass media • Culture • Social networks that influence the opinion of ordinary citizens • Social and information policy, history • Information sphere, scientific and educational spheres • Information • Information, political, economic, cultural • All sectors • Mass media, education, popular culture • Political • informational

	• Media, politics • Economy (investments); international relations, culture and media • Economy, transportation • Information, energy, military domain
Master's degree students of higher education	• Energy, education, defense • Information in most industries • Calaborators in the supreme and central executive authorities • Political systems using disinformation • Culture, religion • Media • Information industry, military, social stability • The nation's mentality, which includes national memory and the perception of Ukraine as a state. Most state institutions, except for cyber transformation • Every industry is vulnerable if society does not protect its culture. Because culture is the root from which everything else grows. And yes, I say this not only as a museum director, but also as a person who understands quite well what countering hybrid threats really means. • In my opinion, the greatest impact of hybrid threats today is observed in the areas of information security, culture, and education. Information attacks are aimed at manipulating the public consciousness, undermining values and trust in state institutions. In the cultural sector, they pose a risk of losing national identity through disinformation and distortion of history. The education sector is also vulnerable, as it shapes future generations, and any impact on this area can have lasting consequences for the state.
Bachelor's degree students of higher education	• Information space • Society, politics
PHD students	• All industries are under threat • Mass media, Internet resources • Agro • Social • Information technology, industry, energy • information • cyber defense, economy, media, logistics • culture, domestic/foreign policy, media, religion, defense, justice
Representatives of the admin staff	• information sphere • ICT, public administration • security, information, academic education • In the field of hybrid operations, one of the key areas is culture, cultural and civilizational values • Mass media, social and communication platforms • government, information space, theater of operations • National security • Culture and art, economy, education • Media, economy and defense
Other categories	• in all industries • Culture • Social networks • Information industry • war, economy, media • MEDIA

According to the results of the survey, the areas in which, according to the respondents, the greatest impact of hybrid threats were identified. Among them, the most frequently

mentioned, regardless of the category of respondents, were identified: economy, media, ICT, education, transport, and military industry.

The results of the answer to the question "Can higher education institutions, in your opinion, counteract the emergence and spread of the impact of hybrid threats?" are shown in Fig. 17.

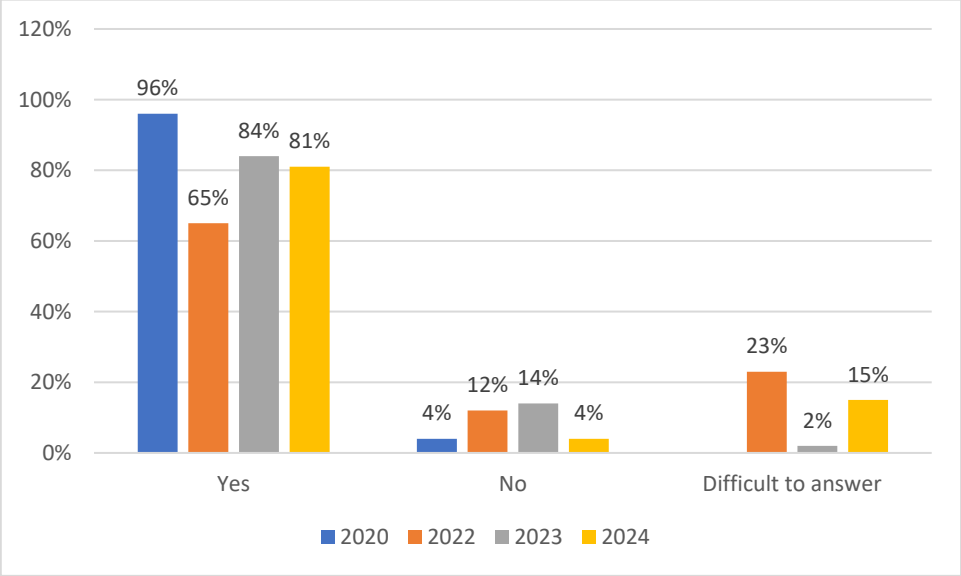

Fig. 17. The results of the answer to the question "Can higher education institutions, in your opinion, counteract the emergence and spread of the impact of hybrid threats?"

The majority of respondents answered in the affirmative. This confirms the effectiveness of the WARN project implementation.

The results of the answer to the question "Would you like to personally take a course on combating hybrid threats?" are shown on Fig. 18.

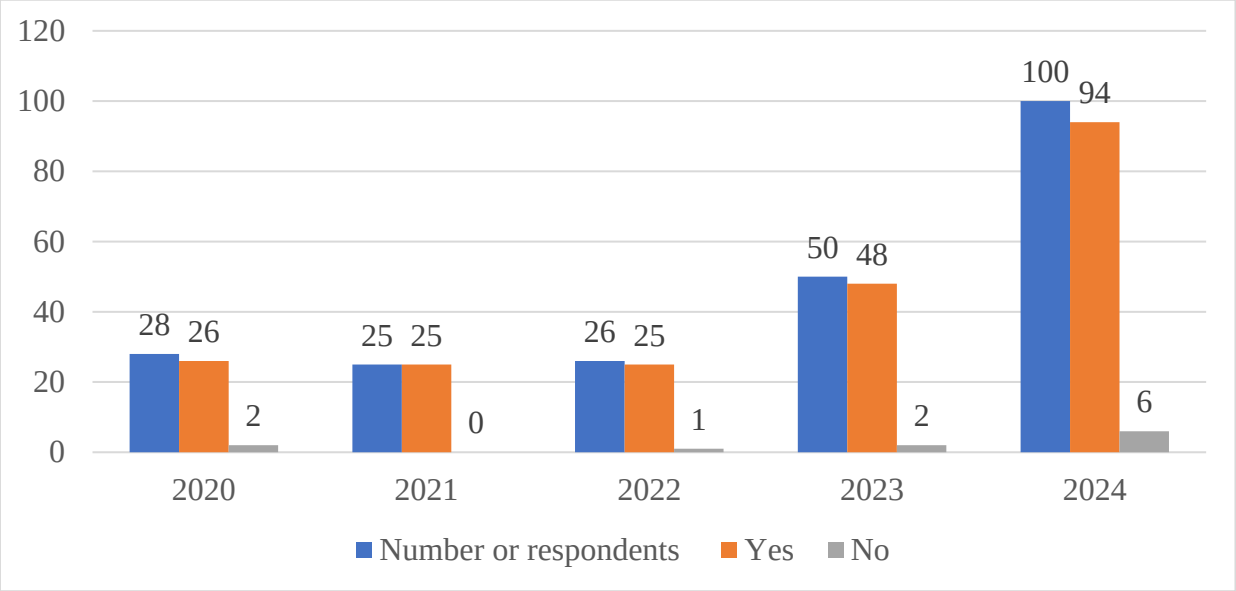

Fig. 18. The results of the answer to the question "Would you like to personally take a course on combating hybrid threats?"

The vast majority of respondents answered in the affirmative. This confirms the effectiveness of the WARN project implementation.

Respondents also answered the question " What knowledge/skills would you expect from such a course?" The results are grouped as a Table 3.

Table 3 - What knowledge/skills would you expect from such a course? (the survey at the conference 2024)

Respondents	Answers
Representatives of the scientific and pedagogical staff	• Development of congruent flexibility and ability to argue responses to hybrid threat • Practical skills in identifying hybrid gassing, skills in countering it • Understanding of my personal contribution to such an important cause, counteracting and helping to fight our common enemy • Tips • Modern methods of countering hybrid threats, media literacy, financial literacy • Analytical: recognizing hybrid threats, critical thinking, risk assessment; and practical: communication skills, cybersecurity, crisis management; and soft skills: teamwork and adaptability • Practical application • Tools for influencing the student audience • learning to resist hybrid threats • Methods of counteraction • Understanding hybrid threats: The basics of hybrid threat theory, their characteristics and examples (military, information, economic). Analysis of information campaigns: Skills in media analysis, detecting disinformation, recognizing manipulative techniques. Cybersecurity: Fundamentals of information systems protection, methods of preventing cyber attacks. Social psychology: Understanding the behavioral aspects that can be used to

	• Improving personal cyber security • Protection of personal information, countering hybrid threats • Stress tolerance, ways to overcome threats, especially the issue of returning Ukrainians to their homeland • When you know, it is easier to react to the situation • Personal involvement • Countering threats in the social and financial spheres • Develop critical thinking skills • Ability to analyze and counter hybrid threats. Understand what tools are available to minimize hybrid threats • Expand experience in mechanisms for identifying, detecting and countering hybrid threats at the business level • How to effectively prevent hybrid threats and be able to recognize their targets • More information • Ability to recognize hybrid threats, practical skills to counter hybrid threats • Find out more details on this topic • Learn to identify threats in messages • Practical measures and mechanisms to prevent impacts at the level of the individual and society • Application of innovative tools to counter hybrid threats • To understand where the true information is • Acquire some basic skills to recognize hybrid threats • To counteract them • What is the difference between hybrid threats and other threats and how to detect them before they become active? • Practical actions to counter threats • Understanding the problem of hybrid threats and their essential features, as well as how to counter them in various spheres of life • Knowledge of the principles of information hygiene. Identification of hidden hybrid threats • Detect, identify and classify hybrid threats, and respond to them adaptively • Recognize disinformation and manipulation in the media. Development of counteraction strategies. Legal aspects of counteraction. • The impact of hybrid threats on modern national security in Ukraine • Psychological support • To counter hybrid threats • Ability to recognize threats • Effective ways to counteract • Analysis of cultural and intercultural aspects that can be used in hybrid operations. • Methods of counteraction • Training, practical • Preventing hybrid threats • Awareness of the realities of today • Related to recognizing, analyzing and countering hybrid threats • Gain more knowledge on how to counter hybrid threats • Understand the terminology • Expand your knowledge • About changes in this area • Skills to identify such threats • Mechanisms of counteraction and updating of tools and methods of hostile influence • Psychological resilience • Counteracting social divisions
Master's degree students of	• Detecting and predicting their occurrence at an early stage. Eliminate them quickly. • Distinguish black from white, increase critical thinking • First of all, develop your own critical thinking

higher education	• Methods of counteracting psychological influence and manipulation • Analysis of information • Practical knowledge of how to counter hybrid threats. Skills that I could implement in my life, both independently and possibly in the future in my position • Knowledge and peace of mind that there is a plan formed on our actual conditions and not calculated from European experience that is not entirely relevant, skills to reassure the public that sees problems but also knows the answers, or at least can characterize possible ways to overcome them. Skills to adopt and cultivate concepts that are both culturally durable and incompatible with hostile narratives • Learning how to protect oneself from hybrid threats • I am answering this question with great interest, because the course on countering hybrid threats at National Academy of Managerial Staff of Culture and Arts has the potential to become one of the most important today. So, let me share my expectations regarding the knowledge and skills it should provide. First of all, the course must teach students the basic art of recognizing propaganda. For example, how not to confuse "cultural dialogue" with an attempt to seize heritage. Or how to understand from the first lines of an article that someone is trying to make Ukrainian art part of the "Russian world." The skills of recognizing fakes, manipulations and, of course, the classic "we are brothers" are a must-have. Secondly, we need crisis management skills. After all, any museum worker will confirm that if you know how to evacuate artworks under fire, you are ready for any crisis. Practical exercises can be included in the course, for example, how to protect the collection from a "hybrid" attack in the style of "we came to see peacefully, but they took out Repin." Third, it is necessary to teach modern technologies. Digitization, cloud services, and database cybersecurity are the real weapons of the 21st century. It would be great if the course taught, for example, how to set up a multi-level security system for an electronic catalog so that it is not hacked by a "friendly hacker." And, of course, effective communication skills. In a world where every post can influence international politics, students need to be taught how to run social media pages properly. After all, what could be more important than explaining in a few words why Ukrainian culture not only survives but thrives, even under fire? Last but not least, the course should develop strategic thinking. How to create a long-term program of cultural resistance? How to combine art, diplomacy and security into a single strategy? These are the questions that future students of the course should know the answers to. So, to summarize, I expect the course to be not only informative but also full of practical exercises. After all, what could be better than students who not only know what hybrid threats are, but also know how to overcome them on a scale worthy of cultural diplomats? • From a course on countering hybrid threats, I would expect knowledge of the main methods of information attacks and manipulations, as well as the skills to detect and neutralize them. In addition, it is important to receive practical recommendations on how to protect cultural heritage from disinformation threats and skills to create information campaigns to raise public awareness. This would help to counteract the challenges facing the cultural sector more effectively.
Bachelor's degree students of higher education	• Detailed consideration of the problem • Media literacy, cybersecurity, critical thinking
PHD students	• What actions and knowledge are needed to counter hybrid threats! • Practical skills • Ability to identify hybrid threats, tools for countering them • Protection against manipulative surfacing • Knowledge of what this phenomenon is, skills to counter it • Ability to identify such threats and how to counter them
Representatives of the admin staff	• Knowledge of the basics of international and national security in the context of hybrid threats • Improve skills in countering hybrid threats • Countering and preventing hybrid threats • "Hybrid warfare" and methods of its conduct, taking into account the current stage of social development.

	• Knowledge of the specifics and types of hybrid threats in the field of education and culture • Skills of recognition and counteraction • Effective counteraction to hybrid threats • Countering hybrid threats
Other category	• Combating hybrid threats • How to counter hybrid threats • Ability to recognize means of influence • Definition, means of counteraction • Increasing knowledge and awareness, ability to counteract disinfection

The vast majority of respondents noted that mastering the course on combating hybrid threats expects to receive relevant information on this topic, learn to recognize hybrid threats, develop effective tools and mechanisms to response to hybrid threats.

Respondents also answered the question " What actions do you think are the most effective today in countering hybrid threats at various levels?" The results are grouped as a Table 4.

Table 4 - What actions do you think are the most effective today in countering hybrid threats at various levels? (the survey at the conference 2024)

Respondents	Answers
Representatives of the scientific and pedagogical staff	• LLL educational courses • Educational events (seminars, workshops, thematic games) • Public policy and public administration • Lectures • Cybersecurity of critical infrastructure, continuous monitoring and threat detection, education and training for the public and civil servants, information security and countering disinformation, modernization of defense structures and preparation for hybrid threats, diplomacy and international cooperation • Media literacy, digital hygiene, awareness raising, independent media and fact-checking, civic education; creation and development of specialized bodies to counter hybrid threats, providing them with the necessary resources and powers. Cybersecurity - protection of state information systems, critical infrastructure, development of the national cybersecurity system. • Informing • Constant work with students • Ability to recognize them • Hold more events to spread the word • Strengthening cybersecurity, education and awareness • Hybrid threats pose a complex and multifaceted challenge that requires a comprehensive and coordinated approach to countering them by states and international organizations • Current measures are effective • The most effective measures to counter hybrid threats at different levels can be classified as follows: - State level (strengthening national security, increasing the resilience of state institutions) - International level (cooperation with international organizations, economic sanctions) - Civil society and information space (increasing information resilience, strengthening national identity and social unity) - Cybersecurity (developing cyber defense, monitoring cyber threats) - Economic level (strengthening economic resilience) - Local level (strengthening regional authorities, developing local

	community) - Cultural level (studying the true history of Ukraine, compulsory knowledge of the Ukrainian language, introduction of national traditions)” • More awareness and cohesion is needed • Educational activities • Educational work with the population, work of special national security agencies, national banks • A comprehensive state policy is needed • Trainings • Popularization of the problem of hybrid threats at the state level • Educational activities (training) and cross-domain communication • Preserving and protecting personal data; ensuring information security at the national and international level; making informed management decisions taking into account the issues of European and Euro-Atlantic integration in the context of preventing and countering hybrid threats; using the legislation of Ukraine on information security and cybersecurity in the course of official activities; using approaches to defining information security; assessing potential threats that may arise when working with information • Timely informing the population about possible threats, adapted courses of academic disciplines, workshops, trainings, discussion of problematic issues • Regulatory documents • Cyberpolice and security • Education, critical thinking and development of effective approaches to personal information hygiene • Education • Outreach to the public • Public education, anti-propaganda, • Implementation of national security strategies; media engagement • Critical thinking • A set of different measures - cyber defense, education, security • Conferences, knowledge sharing and utilization of • Education, national security, military • Actual actions against those who spread and promote these threats • Possibly cybersecurity, information policy, military • Special trainings, blocking of propaganda content • Raising awareness of the dangers of hybrid threats at all levels • Comprehensive approaches that include preventive measures (education, training), technical solutions (cyber defense, monitoring), and rapid response (crisis management, international cooperation). • Public awareness • Psychological support • Civic education and science • Identification of threats • Videos on the Internet • Understanding the impact of hybrid threats on the economy, politics, media and society. • Updating knowledge and applying countermeasures by all segments of the population, including pensioners • Online trainings, seminars, quests, lectures • Building resilience of society, international cooperation, information security • Accurate information • State counteraction programs, educational activities • Workshops • Awareness • Webinars, trainings • Education and creation of effective filters • Strengthening control over cyberspace, development of national cyber defense tools

	• Recognizing and identifying hybrid threats on the basis of the “informed-armed” principle, increasing the resilience of society
Master's degree students of higher education	• Informing and preventive methods • Combating corruption, which is a breeding ground for hybrid influence • Maximum rotation of corrupt officials to the frontline and total propaganda of Ukrainianness in Ukraine and abroad. • International cooperation • Control over the media, especially over anonymous telegram channels • Online events (any informational), performances (any: dance, entertainment, informative), modern exhibitions/museums (to show Ukrainian culture, history) • Events that not only frighten in scale and reveal the effectiveness and diversity of hybrid threat campaigns, but also formulate fundamental responses to challenges, for example, events related to national memory: coverage of the Holodomor events confirms the fact of genocide against the Ukrainian people, but for an ordinary Ukrainian, such as my great-grandmother (who was an eyewitness), the narrative of sit quietly, do nothing, you can do anything for physical survival (as well as cooperation with the enemy) is a parallel and mirror of pro-Russian narratives. In other words, informing without rethinking and formulating, such as the rise of Zionist movements based on the memory of the Holocaust, only supports hostile narratives. Events that are part of popular culture and are built in its conditions and factors (Marketing, Profitability, Popularity, Quality) but carry a certain ideological context are the most effective in countering them. In my opinion, public initiatives and actions created under the control and inspiration of non-governmental patrons are more effective than regulated and quantitatively oriented specific events of the mini-cult. The sculpture and musical performance I'm fine from Burning Man, the National Selection for Eurovision, Rethinking through fashion and advertising by a large number of private “Actors” in my opinion voice more and wider necessary narratives than conversations at meetings and forums • Let's start with the local level. The most effective measure is, of course, a culture of awareness. For example, instead of letting people believe in another fake “friendship of nations,” give lectures about the true origin of our masterpieces. Quests in museums with tasks like “find a fake in a propaganda text” are a great start. At the regional level, events should be larger. Here I would suggest the creation of coordination centers for the protection of cultural heritage. For example, combining the efforts of museums, universities, and volunteers to document and digitize collections. This is not just effective, it is also beautiful - the preserved paintings will never become the “property” of the occupiers. Legislative initiatives are certainly needed at the national level. For example, creating a separate fund to support cultural projects in times of crisis. Why doesn't the state provide museums not only with security guards but also with cybersecurity experts? When databases are protected, hybrid threats become less effective. Cultural diplomacy works at the international level. Organizing exhibitions of Ukrainian art in major capitals of the world is not only a countermeasure to hybrid threats, it is a real diplomatic breakthrough. The more the world knows about our culture, the less chances the enemy has to appropriate it. I would also like to emphasize the use of modern technologies. Why not create an international platform to document crimes against culture? An interactive map of the destruction, data on destroyed monuments and stolen exhibits is not only an evidence base, but also a powerful signal to the world. And, of course, the main thing is cooperation. Successful counteraction to hybrid threats is possible only when all levels work in sync. From a local activist giving a lecture at the National Academy of Managerial Staff of Culture and Arts to an international exhibition at the Louvre, every action must be part of a larger strategy. So, to answer the question, measures are effective when they are systematic, multilevel and based on an understanding of the importance of culture as the basis of national security. Because, as experience shows, protecting a Ukrainian painting or book is protecting the Ukrainian nation. • In my opinion, the most effective measures to counter hybrid threats are to strengthen information security by creating national media platforms and media literacy programs for citizens. At the community level, it is important to implement local initiatives to raise awareness of hybrid threats, as well as to intensify cultural and educational activities that will help strengthen national identity. At the state level, it is necessary to ensure clear coordination between the authorities, civil society institutions, and international partners to respond promptly to challenges.

Bachelor's degree students of higher education	• Dissemination of truthful information • Cybersecurity, countering disinformation, critical thinking
PHD students	• Measures to unite society, measures aimed at security and protection of the population, economic solutions • Educational activities • Information support • Raising awareness and education, Strategic communication • Countering disinformation and information manipulation • education • at the state level - relevant services, for children - education • conferences/seminars of cultural, cultural-religious, business events with the involvement of government officials
Representatives of the admin staff	• Information warning and counteraction to hybrid threats • activities of educational institutions • legislation and special services • Specialized software tools and services for collecting and analyzing information can be used to help identify threats and take timely measures to counter them • Special seminars, special trainings, development of educational programs • Informing the public, training of responsible persons • Educational activities to identify and counter hybrid threats • Seminars, workshops • Cyber defense
Other category	• Cultural and educational mass • Measures to build resilience to counter hybrid threats • Information space • Public awareness of the realities of life • Educational activities, training of professionals • At the public level - educational programs and development of critical thinking, building trust in the state

The responses confirmed that all categories of respondents need to increase awareness to counter hybrid threats. The respondents' answers confirmed that WARN's project activities to raise awareness should be continued, as the issue is very relevant and necessary.

Feedback analysis

To evaluate the conference and its impact, respondents were asked to answer the following questions according to the scale below, where 5 is strongly agree and 1 is strongly disagree (Fig. 19):

1. Did you receive useful information during the Workshop?
2. The results presented are clear and understandable.
3. I am sure that the target groups will learn a lot from the materials presented.
4. I feel motivated to apply the presented materials in my practice.
5. I will share the information with my colleagues

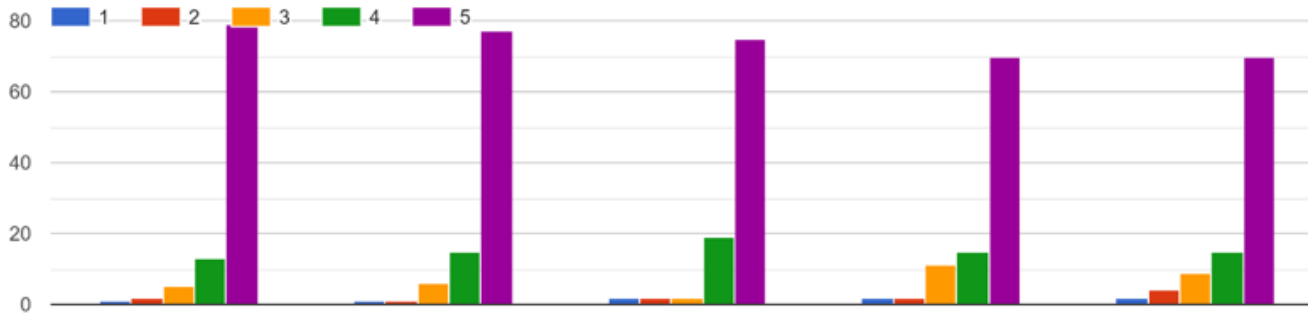

Fig. 19. The results of the answer to the five questions

On the question «Did you receive useful information during the Workshop?» 79 respondents gave the maximum score.

The statement «The results presented are clear and understandable» was given the highest score by 77 respondents.

The statement «I am sure that the target groups will learn a lot from the materials presented» was given the maximum score by 75 respondents.

The statement «I feel motivated to apply the presented materials in my practice» was given the maximum score by 70 respondents.

The statement «I will share the information with my colleagues» was given the maximum score by 70 respondents.

The results confirmed the quality of the preparation and holding of the Fifth International Scientific and Practical Conference "Management and Administration Responses to Hybrid Threats".

Below are some of the feedback we received.

«The anniversary conference on countering hybrid threats demonstrates outstanding achievements in the educational and scientific fields in developing tools for the formation of a hybrid security platform. An incredibly powerful community, which is a great privilege and honour to be a part of».

«It was a great event, allowing to get up-to-date information on hybrid threats and to get acquainted with the results of the WARN project research».

«I am sincerely grateful for the incredible experience, for your hard work»

«Many thanks to the organizers for their professionalism!»

«We look forward to further cooperation»

«Everything was organized at the highest level, efficiently and frankly»

«Thank you for the interesting and useful material. I hope to participate in your events next year»

«Hybrid threats are a hot topic»

«Only gratitude for the high level of the event»

«I wish to move forward and implement the proposed mechanisms systematically and continuously»

«Thanks to the wide representation of various domains, the conference highlighted the truly complex and comprehensive hidden nature of hybrid threats, where parties, tours, refugees, charitable activities, etc. can be used as an attack tool. I thank the organizer for the excellent presentation of this issue»

«An interesting event as a result of the work of teams from different universities, which allowed us to see the phenomenon of hybrid threats from different angles»

«Interesting content for the audience of both generalists and narrow specialists»

«In-depth reports by representatives of various professional fields allowed us to see the complexity and multidirectionality of this problem. Thank you»

«Thank you for the clear and useful content. This is a great example of cooperation between different sectors of public life in the fight against the aggressor»

«There should be more projects like this involving NGOs»

«I would like to express my sincere gratitude to the organizers for the high level of the conference and the relevance of the topics raised! It is very important that such events provide an opportunity to discuss the challenges of hybrid threats and find practical ways to overcome them. It was extremely useful to hear the opinions of experts and share my own ideas. I hope that such initiatives will continue in the future!»

«Human resilience to hybrid threats can be enhanced by strengthening trust in government institutions and the media»

«I wish you success!»

The feedback analysis confirmed that the WARN environment, created during the project implementation, will continue to function and develop in order to enhance national security and overcome the lack of security services that has arisen due to the emergence of hybrid threats.

Conclusions

The results of the surveys were interesting and showed the need to disseminate information about hybrid threats in society and to develop ways and mechanisms to counter these threats. The results confirmed the growing awareness of the conference

participants about the terminology of hybrid threats, the need to introduce courses on countering hybrid threats into the educational process, and the increased interest of respondents in expanding their knowledge and gaining practical skills in countering hybrid threats.

Higher education institutions of Ukraine, through the introduction of relevant academic disciplines, the organization of advanced training courses and other events, should create effective means to explain the nature, inform about hybrid threats, opportunities and ways to prevent them, as well as minimize the negative consequences of the impact of hybrid threats.