Syllabi of New Courses on Countering Hybrid Threats

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

Disclaimer

This project has been funded with support from the European Commission.

This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein.

Project information

Academic Response to Hybrid Threats (WARN) aims to renew the different curricula by introducing unique content that builds awareness of hybrid threats and innovative gamified teaching methods that proactively provide skills and competencies to tackle complex threats. It is a five-year project funded under the EU's Erasmus+ programme. More information can be found here: warn-erasmus.eu

Project Partners

University of Jyvaskyla (Finland)
Universidade de Coimbra (Portugal)
ECAM-EPMI Graduate School of Engineering (France)
Tartu Ulikool (Estonia)
Kharkiv National University of Radio Electronics (Ukraine)
Ukrainian Catholic University (Ukraine)
State University of Infrastructure and Technologies (Ukraine)
National University of Ostroh Academy (Ukraine)
Kharkiv Regional Institute of Public Administration of V. N. Karazin Kharkiv National University (Ukraine)
State Higher Education Institution "Donbas State Pedagogical University (Ukraine)
National Academy of Managerial Staff of Culture and Arts (Ukraine)
Ministry of Education and Science of Ukraine (Ukraine)

TABLE OF CONTENTS

1. INTRODUCTION

This document contains the syllabuses of the new courses developed by seven Ukrainian universities to modernize the curricula and adapt the master's program profiles to focus on countering hybrid threats.

The modernized master's programs were launched in the 2022/2023 academic year, implementing the syllabuses in their initial version (version 1.0).

The current version 2.0 of this document reflects updates that include:

- Reviews and feedback from EU experts—members of the Project Expert Board—received in response to the first version and during visits to partner EU universities;
- Organizational changes among UA partners, including the merging of the Kharkiv Regional Institute of Public Administration of the National Academy for Public Administration under the President of Ukraine (KRI NAPA) with V. N. Karazin Kharkiv National University (KhKNU);
- The transformation of the master's program at KhKNU “Public Management and Administration” into the new master's program “Public Policy and Administration under Conditions of Hybrid Threats,” which was launched within the project;
- The addition of an updated Economics master’s program (by SUIT).

This version of the document is final. It has been developed through continuous beta testing and updates ("fine-tuning") with training materials provided by EU project partners in response to the new security situation and feedback from students and stakeholders.

This document details twelve different versions of a course that is essentially common to all twelve MSc programs. Following this, twelve tailored courses on countering hybrid threats are described in detail.

2 The common course "Hybrid Threats and Comprehensive Security"

Victory in a hybrid war is impossible without a collective and shared understanding of the comprehensive and complex nature of hybrid warfare as well as its logic and patterns. The winning factor is the ability of the nation to offer a unified front that is educated and resilient to unforeseen challenges. Thus, all decision-makers should have sufficient knowledge to see separate threats as elements of a bigger and more complex action and understand the consequences of different incidents across different sectors of society.

To provide a general vision of hybrid threats, we added a basic course to each master's program. One may note that the syllabuses in the first section are similar in structure, recommended literature, etc. This reflects the common unified approach developed by the project team to detect, identify, and classify hybrid threats and react effectively. It also serves the need to establish a common language between experts from various domains to address complex scenarios in collaboration adequately.

This is a meta-level overview course designed to:

- to teach decision-makers at all levels to detect, identify, and classify Hybrid Threats;
- to teach them to assess singular threats in their own domain/responsibility area as elements of more considerable action;
- to uncover the level and complexity of interdependencies between various Hybrid Threats;
- to give them an understanding of the need for integrated adaptive responses joined by actors from various domains.

The master's programs share the same structure for the course but differ in the specific features of their delivery. All UA partners install this course into existing programs, adapting the general structure of the course to their professional context and offering their organization of classes and a specific system of tasks. The Course Objectives also vary due to the specifics of each master's program and learning outcomes.

2.1. NURE (P5): Master Programme on Management of Financial and Economic Security

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security** (Hybrid Threats and Complex Security)
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	073 Management
3	Type and the title of the study program	Master Programme on Financial and Economic Security Management
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian, English
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 30 hours, practical classes – 20 hours, consultations – 10 hours, independent work of students – 90 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	Provide the knowledge and skills needed to understand, analyze and respond to hybrid threats in professional activities and societal life
11	Learning outcomes	● To consider critically, to select and use the necessary scientific, methodological and analytical tools for management under unpredictable conditions; ● to identify the problems of the organization and to justify methods of solving the problems; ● to have the skills of decision making, justification and implementation of management decisions within unpredictable conditions taking into account the requirements of the current legislation, ethical aspect and social responsibility; ● to demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats.
12	Course annotation (content)	Module 1. The nature of hybrid threats Topic 1. Asymmetry, hybrid threats and security. Topic 2. Conceptual model for Hybrid Threats. Module 2. Landscape of Hybrid Threats Topic 3. Domains and tools of hybrid threat activity. Topic 4. Dynamics of hybrid threats. Module 3. Countering hybrid threats. Topic 5. Resilience is a key safety property. Topic 6. Basics of protection.
13	Students performance evaluation	Accumulating grades for the course: ● workshops (5 practical classes) – 10 points,

		● master class "Visualization of hybrid threats" (1 practical class + independent work of students) – 10 points, ● research on Filter Bubbles (1 practical class + independent work of students) – 20 points, ● Intellectual hybrid (human + AI) sparring (2 practical classes) – 20 points ● exam – 40 points. Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	The policy of academic integrity among applicants at NURE provides advice on the requirements for implementing written works, emphasizing the principles of independence, correct use of information from other sources and avoidance of plagiarism, as well as rules for describing sources and citations. The content of the discipline is updated at the end of the previous semester at the initiative of the leading lecturer, considering the educational and scientific interests of students. The content of the educational component is reviewed and updated annually, considering the results of a survey of stakeholders, discussed at meetings of the department and approved by the head of the support group of the specialty. The leading lecturer determines what modern practices and scientific achievements should be used in the educational process.
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE, https://www.hybridcoe.fi/ Glossary of hybrid threats, https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985 Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023. 124 p. doi:10.2760/37899 MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p.
16	Specific equipment, hardware and software for the course	The specialized educational FESM laboratory is a component of the interfaculty NURE Hub on countering hybrid threats and also is a part of the trans-sectoral academic environment countering hybrid threats.

		In 2021, FESM Lab was equipped with powerful computer hardware totally for more than 350 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Economic Cybernetics and Management of Economic Security of. 204i, 201i. Tel. +38(057)7021490, https://eces.nure.ua/
18	Teacher(s) – syllabus designer(s)	Dr. Svitlana Gryshko, PhD, svitlala.gryshko@nure.ua

2.2. NURE (P5): Master Programme on Systems of Artificial Intelligence

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	122 Computer science
3	Type and the title of the study programme	Master Programme on Systems of Artificial Intelligence
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 30 hours, seminars/practical classes – 20 hours, consultations – 10 hours, independent work of students – 90 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	Provide the knowledge and skills needed to understand, analyze and respond to hybrid threats in professional activities and societal life
11	Learning outcomes	● To demonstrate the ability to participate in teamwork and use collective development or research tools. ● To be capable of communicating with people who are not professionals in the field of computer science in order to identify their needs for computerization of the processes where they are involved. ● To take into account the socio-economic aspects of the project in the context of the development or research task, in particular, the consistency of technical progress and ethical standards ● To analyze current global trends in computer science. ● To demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in trans-sectoral collaboration.
12	Course annotation (content)	Module 1. Introduction to Hybrid Threats Topic 1. New security landscape, war and peace; Topic 2. Hybrid threats - history, definitions, essential features: asymmetry, synchronized attack package, creativity and ambiguity, sub-threshold activities Module 2. Conceptual model of hybrid threats. Topic 1. The Landscape of Hybrid Threats: background, elements and structure of the model.

		Topic 2. State and non-state actors, their use in hybrid influencing. Module 3. The domains of malicious actions Topic 1. PMESII spectrum: information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, and infrastructure domains. Topic 2. Cyber domain and AI Security. Module 4. Tools and phases of hybrid threat activity Topic 1: System of tools of hybrid influencing; operations against infrastructure; cyber espionage and cyber operations; electronic operations; economic, military/paramilitary, sociocultural; tools in public administration; legal, intelligence-diplomatic, information-analytical, and media tools. Topic 2. Critical functions and vulnerabilities, decision-making under threat, operations against critical infrastructure. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. Module 5. Countering hybrid threats Topic 1. Comprehensive security concept (based on the Finnish model example). CORE Model. Building resilience (including cases from trainings in the EU, e.g., Danske bank money laundering scandal), Holling`s adaptive cycle, panarchy. Topic 2. Building a strategy for countering hybrid threats: detecting (monitoring vs discovery), deterring by denial, deterring by punishment, responding.
13	Students performance evaluation	Accumulating grades for the course: ● workshops (1 practical session: case study) – 20 points, ● master class - 2 practical sessions: ○ visualizing hybrid threats - 20 points; ○ visualizing a counter-strategy for hybrid threats – 20 points; ● strategic wargaming (1 dilemma game “Ukraine before accession to EU” developed under the supervision of TNO Lab) – 20 points, ● brainstorming (1 practical session on the glossary for hybrid threats) – 20 points Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Academic integrity is a fundamental feature of the educational process. The principles of academic integrity are described in the Regulations on the Fight against Academic

		Plagiarism in NURE and the Regulations on the Organization of the Educational Process in NURE, p. 5.8. Evaluation of students' performance is a tool to control the quality and to measure the achievement of the intended learning outcomes. Grades are based upon in-class (online) participation, learning activities, and assignments. The point values associated with each activity are delineated in the student evaluation section of this document. The criteria used in grading each assignment are discussed in class and are specified and provided in written form at the beginning of the course. Grades are assigned on the basis of accumulated points. All practical and lab works are completed individually in class. The presence of a student in class is a prerequisite for obtaining the maximum grade. The absence implies a 20% score reduction; the absence and the completion of the task after the deadline imply a 30% reduction of the grade. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE, https://www.hybridcoe.fi/ Website of EU East StratCom Task Force (ESTF), https://euvsdisinfo.eu/ Glossary of hybrid threats, https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985, JRC123305 MCDC (2017), Understanding Hybrid Warfare. Available at: https://www.gov.uk/government/publications/countering-hybridwarfare-project-understanding-hybrid-warfare MCDC (2019), Countering Hybrid Warfare, 2019. Available at: https://www.gov.uk/government/publications/countering-hybridwarfare-project-understanding-hybrid-warfare Sweijs, T., & Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019. Sweijs, T., Zilincik, S., Bekkers, F., & Meessen, R. (2021). *A framework for cross-domain strategies against hybrid threats*. Den Haag, NL: Hague Centre for Strategic Studies.

16	Specific equipment, hardware and software for the course	The specialized educational AI laboratory is a component of the interfaculty NURE Hub on countering hybrid threats, and also is a part of the trans-sectoral academic environment countering hybrid threats. In 2021, AI Lab was equipped with powerful computer hardware totally for more than 420 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Artificial Intelligence (AI), http://ai.nure.ua, d_ai@nure.ua
18	Teacher(s) – syllabus designer(s)	Dr. Mariia Golovianko, PhD, mariia.golovianko@nure.ua

2.3 UCU (P6): Master Programme on Public Administration

№	Field name	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	281 Public Administration
3	Type and the title of the study programme	Master Programme on Public Administration
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 24 hours, practical classes – 28 hours, consultation – 8 hours, independent work of students – 90 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	Year 2, Semester 1
10	Course objectives	Provide the knowledge and skills needed to understand, analyze and respond to hybrid threats in professional activities and societal life
11	Learning outcomes	Understand the complex nature, complexity, logic and patterns of hybrid threats in public administration Understand the peculiarities of the formation of viability and adaptability in environments exposed to hybrid threats Make informed decisions and use modern communication technologies to counter hybrid threats Carry out professional activities, in particular, to ensure the national security of the country Ability to develop strategic documents for the development of socio-economic systems at the highest, central, regional, local and organizational levels as one of the tools to respond to hybrid threats Analyze the nature and evolution of hybrid threats: Students will be able to explain the historical context, key features, and areas sensitive to hybrid threats, particularly in the domains of security, public administration, and political processes. Evaluate risk assessment methodologies: Students will be able to apply risk matrices and other analytical tools to assess and mitigate the risks posed by hybrid threats, while understanding the principles of media literacy, propaganda, and information dissemination. Propose strategies for countering hybrid threats: Students will be able to develop informed strategies to detect and counter hybrid threats, drawing on global best

		practices, fact-checking efforts, and Open Source Intelligence (OSINT) frameworks, while balancing security with civil liberties.
12	Course annotation (content)	Module I. Asymmetry, hybrid threats and security: History and key features of hybrid threats. Areas sensitive to the challenges pos xoed by hybrid threats Module II. Asymmetry, hybrid threats and security (*continued*): Risk and risk assessment. Risk matrix and its application in the analysis of hybrid threats Module III. Domains of hybrid threats (*selected*): Fundamentals of critical thinking and media literacy. The evolution of propaganda. Principles of dissemination of information threats in traditional and social media. Culture as a tool of hybrid influence Module IV. Domains of hybrid threats (*selected, continued*): Impact of hybrid threats on public administration and political processes. Protect the process of collecting and counting votes during e-voting. Security of personal data of citizens. Pseudo-activists and imposing an alternative agenda Module V. Tools for counteracting hybrid threats: Ways to counter hybrid threats. The role of the state in detecting and counteracting hybrid malignant influences. Institutes and networks. Activities of fact-checkers and Open Source Intelligence (OSINT) activists and OSINT framework Module VI. Fundamentals of Defense: International Experience in Public Combating Hybrid Threats: Global Lessons and Local Cases. Prospects for confronting new threats. Balance of protection of citizens and inviolability of their freedoms
13	Students performance evaluation	Accumulation of points in the discipline: workshops (6 practical tasks) - 40 points, team projects (2 team tasks) - 40 points, mini-research (1 on a self-selected topic) - 20 points Maximum number of points - 100 (60 and more - credited, 59 and less - not credited)
14	Quality assurance of the educational process	The course will apply UCU's policies on academic integrity and plagiarism prevention, which can be found at this link: https://bit.ly/3IXhZlz
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE, https://www.hybridcoe.fi/, website of EU East StratCom Task Force (ESTF), https://euvsdisinfo.eu/ Glossary of hybrid threats, https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The

		Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985, JRC123305 MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p. Sweijs, T., & Zilincik, S. (2019). Cross-Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023. 124 p. doi:10.2760/37899 MCDC (2017), Understanding Hybrid Warfare. Available at: https://www.gov.uk/government/publications/countering-hybridwarfare-project-understanding-hybrid-warfare MCDC (2019), Countering Hybrid Warfare, 2019. Available at: https://www.gov.uk/government/publications/countering-hybridwarfare-project-understanding-hybrid-warfare
16	Material and technical, laboratory, and software provision of the discipline	UCU University Newsroom is part of an inter-program Hub for countering hybrid threats, as well as a member of the trans-sectoral environment for countering hybrid threats WARN. In 2021, the newsroom received computer equipment totalling more than UAH 750,000, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). University computer laboratories with appropriate software, UCU library fund
17	Department	School of Public Administration, spm@ucu.edu.ua
18	Teacher(s) - developer(s) of the syllabus	Andriy Berezhansky, berezhanskyi@ucu.edu.ua Taras Zhovtenko, zhovtenko@ucu.edu.ua

2.4 UCU (P6): Master Programme on Journalism

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	061 Journalism
3	Type and the title of the study programme	Master Programme on Journalism
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 24 hours, practical classes – 28 hours, consultation – 8 hours, independent work of students – 90 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	Year 2, Semester 1
10	Course objectives	Provide the knowledge and skills needed to understand, analyze and respond to hybrid threats in professional activities and societal life
11	Learning outcomes	Understand the complex nature, complexity, logic and patterns of hybrid threats in the field of journalism/media communications Understand the peculiarities of the formation of viability and adaptability in environments exposed to hybrid threats Make informed decisions and use modern communication technologies to counter hybrid threats Carry out professional journalistic and communication activities, in particular in order to ensure the national security of the country Critically assess the role of media in the context of hybrid threats: Journalism students will be able to identify and analyze the ways in which propaganda and misinformation are disseminated through traditional and social media, while enhancing their critical thinking and media literacy skills. Investigate and report on hybrid threats using advanced research techniques: Students will apply investigative journalism methodologies, including Open Source Intelligence (OSINT) and fact-checking tools, to uncover and report on hybrid threats, ensuring the accuracy and reliability of their reporting. Develop ethical and effective journalistic practices to counter hybrid threats: Students will formulate ethical

		strategies for covering hybrid threats, focusing on the protection of personal data, safeguarding democratic processes such as e-voting, and countering the influence of pseudo-activists and alternative agendas, while maintaining journalistic integrity.
12	Course annotation (content)	Module I. Asymmetry, hybrid threats and security: History and key features of hybrid threats. Areas sensitive to the challenges posed by hybrid threats Module II. Asymmetry, hybrid threats and security (*continued*): Risk and risk assessment. Risk matrix and its application in the analysis of hybrid threats Module III. Domains of hybrid threats (*selected*): Fundamentals of critical thinking and media literacy. The evolution of propaganda. Principles of dissemination of information threats in traditional and social media. Culture as a tool of hybrid influence Module IV. Domains of hybrid threats (*selected, continued*): Impact of hybrid threats on media, communications and political processes. Security of personal data of journalists, communicators and citizens. Pseudo-activists and imposing an alternative agenda Module V. Tools for counteracting hybrid threats: Ways to counter hybrid threats. The role of the state in detecting and counteracting hybrid malignant influences. Institutes and networks. Activities of fact-checkers and Open Source Intelligence (OSINT) activists (OSINT framework) Module VI. Fundamentals of Defense: International Experience in Public Combating Hybrid Threats: Global Lessons and Local Cases. Prospects for confronting new threats. Balance of protection of citizens and inviolability of their freedoms
13	Students performance evaluation	Accumulation of points in the discipline: workshops (6 practical tasks) - 40 points, team projects (2 team tasks) - 40 points, mini-research (1 on a self-selected topic) - 20 points Maximum number of points - 100 (60 and more - credited, 59 and less - not credited)
14	Quality assurance of the educational process	The course will apply UCU's policies on academic integrity and plagiarism prevention, which can be found at this link: https://bit.ly/3IXhZlz
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE, https://www.hybridcoe.fi/ Website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/

		Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985, JRC123305 MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p. Sweijs, T., & Zilincik, S. (2019). Cross-Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p.
16	Specific equipment, hardware and software for the course	UCU University Newsroom is part of an inter-program Hub for countering hybrid threats, as well as a member of the trans-sectoral environment for countering hybrid threats WARN. In 2021, the newsroom received computer equipment totalling more than UAH 750,000, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). University computer laboratories with appropriate software, UCU library fund
17	Department	School of Public Administration, spm@ucu.edu.ua
18	Teacher(s) – syllabus designer(s)	Andriy Berezhansky, berezhanskyi@ucu.edu.ua Taras Zhovtenko, zhovtenko@ucu.edu.ua

2.5 SUIT (P7): Master Programme on Organization Management and Administration

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	073 Management
3	Type and the title of the study programme	Master Programme on Organization Management and Administration
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	4
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 24 hours, seminars/practical classes – 20 hours, independent work of students – 76 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	To form a system of knowledge and skills necessary to perform the organizational, analytical and advisory functions of identifying and countering hybrid threats and ensuring integrated security at the national and international levels.
11	Learning outcomes	● To organize and carry out effective communications within the team, with representatives of different professional groups and in the international context; ● to demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats. ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in transsectoral collaboration.
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI". Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing. Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, and infrastructure domains.

		Module 4. Tools of hybrid threat activity: system of tools of hybrid influencing, operations against infrastructure, cyber espionage and cyber operations, electronic operations, economic, military/paramilitary, sociocultural, tools in public administration, legal, intelligence-diplomatic, information-analytical, media tools. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. Module 6. Basics of protection: history of the issue and basic approaches to countering hybrid threats; comprehensive security concept (based on the Finnish model example); self-assessment; countering; detecting (monitoring vs discovery) of hybrid threats; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats. The comprehensive resilience ecosystem (CORE) model.
13	Students performance evaluation	Type of work (*maximum points)*: current control - *max 80, exam* - *max 20.* Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Adherence to the principles of academic integrity is carried out in accordance with the Code of Academic Integrity of the State University of Infrastructure and Technologies, the Regulations on the system of academic integrity in the State University of Infrastructure and Technologies and the principles of academic integrity. organization of the educational process at the State University of Infrastructure and Technologies, p.4.9. The tool of control measures is a rating assessment of students. Each point is awarded for a specific achievement, a list of which is published at the beginning of the course. During the semester, students "gain" a certain number of points for the results of their work. All practical and lab works are implemented in groups in class. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students
15	Recommended or required reading and other learning resources/tools	Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985,

		https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 Glossary Hybrid Threats / Глосарій з гібридних загроз / упоряд. С.В.Гришко та ін.; за ред. С. Гришко. 2021. 113. https://openarchive.nure.ua/handle/document/16258 Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf Monaghan Sean (Ed.), Patrick Cullen, and Njord Wegge. 2019. MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. 94 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf Cullen, Patrick J, and Erik Reichborn-Kjennerud. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare A Multinational Capability Development Campaign project (2017). 36 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory is a component of the Faculty of Management and Technology of the State University of Infrastructure and Technologies, a member of the trans-sectoral environment for combating hybrid threats WARN. In 2021, the laboratory received powerful computer equipment totalling more than 736 thousand UAH, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE -JP)
17	Department	Department of Management and Public Administration, room 608.
18	Teacher(s) – syllabus designer(s)	Karpenko Oksana, Doctor of Sciences in Economics, Professor, Professor of the Department of Management and Public Administration, karpo_2004@ukr.net Osypova Yevheniia, Candidate of Sciences in Economics, Associate Professor, Associate Professor of the Department of Management and Public Administration, layretta@ukr.net

2.6 SUIT (P7): Master Programme on Software Engineering

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	121 "Software Engineering"
3	Type and the title of the study programme	Master Programme on Software Engineering
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	4
7	Structure of the course (distribution of the types and the hours of the study)	Lectures - 24 hours. Practical - 20 hours. Independent work - 76 hours.
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year (1 course), 1 semester
10	Course objectives	To form a system of knowledge and skills necessary to perform the organizational, analytical and advisory functions of identifying and countering hybrid threats and ensuring integrated security at the national and international levels.
11	Learning outcomes	PH12. Make effective organizational and managerial decisions in conditions of uncertainty and changing requirements, and compare alternatives and change risks. PH18.Understand the complex nature, complexity, logic and patterns of hybrid threats. PH19. Identify and classify hybrid threats and respond effectively to them in intersectoral interaction.
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI". Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing. Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, and infrastructure domains. Module 4. Tools of hybrid threat activity: system of tools of hybrid influencing, operations against infrastructure, cyber espionage and cyber operations, electronic operations, economic, military/paramilitary, sociocultural, tools in

		public administration, legal, intelligence-diplomatic, information-analytical, media tools. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. Module 6. Basics of protection: history of the issue and basic approaches to countering hybrid threats; comprehensive security concept (based on the Finnish model example); self-assessment; countering; detecting (monitoring vs discovery) of hybrid threats; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats. The comprehensive resilience ecosystem (CORE) model.
13	Students performance evaluation	Type of work (*maximum points)*: current control - *max 80, exam - max 20.* Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Adherence to the principles of academic integrity is carried out in accordance with the Code of Academic Integrity of the State University of Infrastructure and Technology, the Regulations on the system of academic integrity in the State University of Infrastructure and Technologies and the principles of academic integrity. organization of the educational process at the State University of Infrastructure and Technology, p.4.9. The tool of control measures is a rating assessment of students. Each point is awarded for a specific achievement, a list of which is published at the beginning of the course. During the semester, students "gain" a certain number of points for the results of their work. All practical work has a group nature and is performed in class. At the end of the course, an anonymous survey of students is conducted to obtain feedback on the usefulness of the proposed material and the complexity of the work.
15	Recommended or required reading and other learning resources/tools	Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985,

		https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 Glossary Hybrid Threats / Глосарій з гібридних загроз / упоряд. С.В.Гришко та ін.; за ред. С. Гришко. 2021. 113 с., https://openarchive.nure.ua/handle/document/16258 Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf Monaghan Sean (Ed.), Patrick Cullen, and Njord Wegge. 2019. MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. 94 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf Cullen, Patrick J, and Erik Reichborn-Kjennerud. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare A Multinational Capability Development Campaign project (2017). 36 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory is a component of the Faculty of Management and Technology of the State University of Infrastructure and Technology, a member of the trans-sectoral environment for combating hybrid threats WARN. In 2021, the laboratory received powerful computer equipment totalling more than 736 thousand UAH, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE -JP)
17	Department	Department of Management, Public Administration and Administration, room 608.
18	Teacher(s) – syllabus designer(s)	Karpenko Oksana, Doctor of Economics, Professor, Professor of the Department of Management, Public Administration and Administration, karpo_2004@ukr.net Osypova Yevheniia, Candidate of Sciences in Economics, Associate Professor, Associate Professor of the Department of Management and Public Administration, layretta@ukr.net

2.7 SUIT (P7): Master Programme Economics (additionally)

№	Name of the field	Course Title: Hybrid Threats and Comprehensive Security
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	051 Economics
3	Type and the title of the study programme	Master Programme on Economics
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	4
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 24 hours, seminars/practical classes – 20 hours, independent work of students – 76 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	To form a system of knowledge and skills necessary to perform the organizational, analytical and advisory functions of identifying and countering hybrid threats and ensuring integrated security at the national and international levels.
11	Learning outcomes	● To communicate fluently on professional and scientific issues in the state and foreign languages orally and in writing. ● To develop socio-economic projects and a system of integrated actions for their implementation, taking into account their goals, expected socio-economic consequences, risks, legislative, resource and other constraints. ● To develop scenarios and strategies for the development of socio-economic systems. ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in transsectoral collaboration.
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI". Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing.

		Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, and infrastructure domains. Module 4. Tools of hybrid threat activity: system of tools of hybrid influencing, operations against infrastructure, cyber espionage and cyber operations, electronic operations, economic, military/paramilitary, sociocultural, tools in public administration, legal, intelligence-diplomatic, information-analytical, media tools. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. Module 6. Basics of protection: history of the issue and basic approaches to countering hybrid threats; comprehensive security concept (based on the Finnish model example); self-assessment; countering; detecting (monitoring vs discovery) of hybrid threats; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats. The comprehensive resilience ecosystem (CORE) model.
13	Students performance evaluation	Current control = max 100 Maximum = 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Adherence to the principles of academic integrity is carried out in accordance with the Code of Academic Integrity of the State University of Infrastructure and Technologies, the Regulations on the system of academic integrity in the State University of Infrastructure and Technologies and the principles of academic integrity. organization of the educational process at the State University of Infrastructure and Technologies, p.4.9. The tool of control measures is a rating assessment of students. Each point is awarded for a specific achievement, a list of which is published at the beginning of the course. During the semester, students "gain" a certain number of points for the results of their work. All practical and lab works are implemented in groups in class. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students

15	Recommended or required reading and other learning resources/tools	Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985, https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 2. Glossary Hybrid Threats / Глосарій з гібридних загроз / упоряд. С.В.Гришко та ін.; за заг. ред. С.В. Гришко. 2021. 113 с. URL: https://openarchive.nure.ua/handle/document/16258 Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf Monaghan Sean (Ed.), Patrick Cullen, and Njord Wegge. 2019. MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. 94 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf Cullen, Patrick J, and Erik Reichborn-Kjennerud. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare A Multinational Capability Development Campaign project (2017). 36 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory is a component of the Faculty of Management and Technology of the State University of Infrastructure and Technologies, a member of the trans-sectoral environment for combating hybrid threats WARN. In 2021, the laboratory received powerful computer equipment totaling more than 736 thousand UAH, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE -JP)
17	Department	Department of Management and Public Administration, room 608.

18	Teacher(s) – syllabus designer(s)	Karpenko Oksana, Doctor of Sciences in Economics, Professor, Professor of the Department of Management and Public Administration, karpo_2004@ukr.net Osypova Yevheniia, Candidate of Sciences in Economics, Associate Professor, Associate Professor of the Department of Management and Public Administration, layretta@ukr.net

2.8 NUOA (P8): Master Programme on National Security

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	25 Military sciences, national security, security of the state border; 256 National security (for certain areas of support and types of activity)
3	Type and the title of the study programme	Master Programme on National security (for certain areas of support and types of activity)
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 16 hours, seminars/practical classes – 14 hours, independent work of students – 120 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	1 year, 1 semester
10	Course objectives	Provide the knowledge and skills needed to understand the role and place of hybrid threats in the context of modern scientific and practical understanding of politics, the political process and the national security of the state.
11	Learning outcomes	● To understand the theoretical bases of the concepts and approaches of the informational and hybrid nature of modern conflicts; ● To demonstrate an understanding of the basic principles, methods and techniques of studying and researching the main characteristics and signs of hybrid wars as a key threat to the security of our time; ● To demonstrate an understanding of the relevance of ensuring the national security of the state in the context of countering modern threats, in particular, hybrid ones; ● To understand the internal and external components of the processes of identifying and countering hybrid threats, their role and importance in the context of protecting the national security of the state; ● To understand the complex nature, complexity, logic and patterns of hybrid threats; ● To demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats; ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in transsectoral collaboration.

		● To demonstrate an understanding of the basic principles and approaches to the use of normal-form games and hybrid warfare simulations in the context of national security; ● To identify, analyse and classify various cyber threats, assessing their potential impact on national security
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI". Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing. Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, and infrastructure domains. Resilience in the context of cyber security. Module 4. Tools of hybrid threat activity: a system of tools of hybrid influencing, operations against infrastructure, cyber espionage and cyber operations, electronic operations, economic, military/paramilitary, sociocultural, tools in public administration, legal, intelligence-diplomatic, information-analytical, and media tools. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. Module 6. Basics of protection: history of the issue and basic approaches to countering hybrid threats; comprehensive security concept (based on the Finnish model example); self-assessment; countering; detecting (monitoring vs discovery) of hybrid threats; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats. Normal-form games in the context of countering hybrid threats.
13	Students performance evaluation	Accumulating grades for the course: ● 7 practical classes – 70 points, ● Scientific essay – 20 points, ● Test – 20 points. Maximum – 100 (61 and more – pass, 60 and less – fail)
14	Quality assurance of the educational process	Procedures for adherence to the principles of academic integrity are regulated by the Regulations on Ensuring the Quality of Educational Activities and the Quality of Higher Education in NUOA and the principles of academic integrity

		set forth in the NUOA Education Regulations and the Code of Academic Integrity The instrument of control activities is the rating assessment of students. Each point is awarded for a specific achievement, a list of which will be published at the beginning of the course. During the semester, students receive points for their performance in each lesson. The presence of a student in each class is a prerequisite for obtaining a 100% grade. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students.
15	Recommended or required reading and other learning resources/tools	Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, doi:10.2760/44985, JRC123305. Aho A., Alonso Villota M., Giannopoulos G., Jungwirth R., Lebrun M., Savolainen J., Smith H., Willkomm E. Hybrid threats: A comprehensive resilience ecosystem. 2023. 120 p. Pat Harrigan, Matthew G. Kirschenbaum, James F. Dunnigan. Zones of Control: Perspectives on Wargaming (Game Histories). Routledge. 2020. 250 p. Merle Maigre. Hybrid CoE Paper 11: Cyber threat actors: how to build resilience to counter them. 2022. 19 p.
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory "Laboratory for Research on Hybrid Threats to National Security" (LRHTNS) is a component of the Educational and Scientific Institute of International Relations and National Security of NUOA and also is a part of the trans-sectoral academic environment countering hybrid threats. In 2021, the educational and research laboratory LRHTNS was equipped with powerful computer hardware totally for more than 350 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Political Sciences and National Security, new campus *Tel.* +38 (03654) 22949, https://www.oa.edu.ua/ua/departments/mizhn/pim_polit/ kafedra.politologii@oa.edu.ua
18	Teacher(s) – syllabus designer(s)	Dr., Zhovtenko Taras Hryhorovych, PhD, Taras.Zhovtenko@oa.edu.ua Konopka Nataliia Olehivna, Associate Professor, PhD natalia.konopka@oa.edu.ua

2.9 NUOA (P8): Master Programme on Political Sciences

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	052 Political Sciences
3	Type and the title of the study programme	Master Programme on Political Sciences
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 16 hours, seminars/practical classes – 14 hours, independent work of students – 120 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	1 year, 1 semester
10	Course objectives	Provide the knowledge and skills needed to understand the role and place of hybrid threats in the context of modern scientific and practical understanding of politics, the political process and the national security of the state.
11	Learning outcomes	● To understand the theoretical bases of the concepts and approaches of the informational and hybrid nature of modern conflicts; ● To demonstrate an understanding of the basic principles, methods and techniques of studying and researching the main characteristics and signs of hybrid wars as a key threat to the security of our time; ● To demonstrate an understanding of the relevance of ensuring the national security of the state in the context of countering modern threats, in particular, hybrid ones; ● To understand the internal and external components of the processes of identifying and countering hybrid threats, their role and importance in the context of protecting the national security of the state; ● To understand the complex nature, complexity, logic and patterns of hybrid threats; ● To demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats; ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in trans-sectoral collaboration.

		● To be able to integrate modern technologies and innovative methods into the process of political analytics to increase its effectiveness ● To conduct a detailed analysis of information operations and cyberattacks, identifying their goals, methods and potential impact on political processes.
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI". Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing. Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, and infrastructure domains. Module 4. Tools of hybrid threat activity: system of tools of hybrid influencing, operations against infrastructure, cyber espionage and cyber operations, electronic operations, economic, military/paramilitary, sociocultural, tools in public administration, legal, intelligence-diplomatic, information-analytical, media tools. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. AI and hybrid threats in the political dimension. Module 6. Basics of protection: history of the issue and basic approaches to countering hybrid threats; comprehensive security concept (based on the Finnish model example); self-assessment; countering; detecting (monitoring vs discovery) of hybrid threats, particularly in cyberspace; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats. Resilience in the context of cyber security.
13	Students performance evaluation	Accumulating grades for the course: ● 7 practical classes – 70 points, ● Scientific essay – 20 points, ● Test – 20 points. Maximum – 100 points (61 and more – pass, 60 and less – fail)
14	Quality assurance of the educational process	Procedures for adherence to the principles of academic integrity are regulated by the Regulations on Ensuring the

		Quality of Educational Activities and the Quality of Higher Education in NUOA and the principles of academic integrity set forth in the NUOA Education Regulations and the Code of Academic Integrity The instrument of control activities is the rating assessment of students. Each point is awarded for a specific achievement, a list of which will be published at the beginning of the course. During the semester, students receive points for their performance in each lesson. The presence of a student in each class is a prerequisite for obtaining a 100% grade. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students.
15	Recommended or required reading and other learning resources/tools	Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 Aho A., Alonso Villota M., Giannopoulos G., Jungwirth R., Lebrun M., Savolainen J., Smith H., Willkomm E. Hybrid threats: A comprehensive resilience ecosystem. 2023. 120 p. Nicolas Mazzucchi. Hybrid CoE Paper 14: AI-based technologies in hybrid conflict: The future of influence operations. 2022. 19 p. Merle Maigre. Hybrid CoE Paper 11: Cyber threat actors: how to build resilience to counter them. 2022. 19 p.
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory “Laboratory for Research on Hybrid Threats to National Security” (LRHTNS) is a component of the Educational and Scientific Institute of International Relations and National Security of NUOA and also is a part of the trans-sectoral academic environment countering hybrid threats. In 2021, the educational and research laboratory LRHTNS was equipped with powerful computer hardware totally for more than 350 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Political Sciences and National Security, new campus *Tel.* +38 (03654) 22949, https://www.oa.edu.ua/ua/departments/mizhn/pim_polit/ kafedra.politologii@oa.edu.ua

18	Teacher(s) – syllabus designer(s)	Dr., Zhovtenko Taras Hryhorovych, PhD, Taras.Zhovtenko@oa.edu.ua Konopka Nataliia Olehivna, Associate Professor, PhD natalia.konopka@oa.edu.ua

2.10 NAMSCA (P9): Master Programme on Cross-cultural Management

№	Field name	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	028 Management of Sociocultural Activities
3	Type and the title of the study programme	Master Programme on Cross-cultural Management
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 10 hours Practical lessons – 30 hours Module - 10 hours Individual work – 100 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1st year / 1st semester
10	Course objectives	- to provide the knowledge and skills needed to understand, analyse and respond to HTs in professional activities and public life. - to form a system of knowledge and skills necessary to do organisational, analytical and consulting functions for the identification and resisting of the HTs and to ensure comprehensive security at the national and international levels.
11	Learning outcomes	LO 1. To find out, analyse and evaluate the information needed to set and solve both professional tasks and the issues of personal development. LO 5. To use an interdisciplinary approach to solve complex tasks and problems of sociocultural activities; LO 6. To analyse and assess risks, make effective decisions on sociocultural activities; LO 9. To present and discuss the results of scientific and applied research, sociocultural strategies and projects in the state and foreign languages; LO 13. To understand and apply in practice theoretical and methodological knowledge on the theory of the sociocultural systems; LO 14. The ability to create a perspective cross-cultural environment with adaptive socio-cultural practices and a system of responding to hybrid challenges. LO 15. To ability to work in the conditions of the transformation processes, caused by hybrid threats.

12	Course annotation (content)	Content module 1: Asymmetry, Hybrid Threats and Security. Decision-making system in the modern security landscape. Historical background and the development of the concept of hybrid threats. Hybrid threats: the essence and main features. 4. PMESII spectrum; «4 + 1 + AI» (land, air, sea, space + cyber + AI). Content module 2: Conceptual Model of Hybrid Threats. Basic principles, structure and tools of the hybrid threat model. State and non-state actors of hybrid threats. Content module 3: Domains of Hybrid Threats. Hybrid threats in an open society: main vulnerabilities (Infrastructure domains, Cyber domains, Vulnerabilities domains in astronomic activities, Economic domains, Military (defence) domains, Cultural domains, Social (civil) domains, Public management domains, Legal domains, Intelligence domains, Diplomatic domains, Political domains, Information domains). Content module 4: Tools of Hybrid Threats. Hybrid threats: instruments and their use. Tools in public management. Legal tools. Intelligence and diplomatic tools. Informational analytic tools. Media tools Content module 5: Dynamics of Hybrid Threats. Main phases and activities of hybrid threats Content module 6. Fundamentals of Resistance to Hybrid Threats. Integrative approach to the resistance to hybrid threats. Complex security conception (Finish model). Main principles of responding to hybrid threats. The EU and refugee challenge. Civil sustainability is fundamental to the formation of a security environment.
13	Students performance evaluation	Forms of Student Control: Evaluation of student's work at practical lessons– 30 points / 18 points. Individual work – 30 points / 18 points. Exam – 40 points / 24 points. Scale of Evaluation: According to the national differential scale – «Excellent», «Good», «Satisfied», «Unsatisfied». According to the ECATS scale: A 90-100, B 82-89, C 74-81, D 64-73, E 60-63, FX 35-59, F 1-34.
14	Quality assurance of the educational process	All participants of the educational process follow the norms of the policy of academic integrity of the NACAM, which is based on the following documents - Code of Academic Integrity and Regulations on the System of Ensuring the Quality of Educational Activities and the Quality of Higher Education in NACAM.

		The main tools of the student control is the rating assessment. During the semester, students get various points for their work at the practical lessons and lectures. The final mark is determined by the common points for exam and students participation in the studying process (lectures & practical lessons)
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/ Website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Світова гібридна війна: український фронт. За ред. Горбуліна В. П. Київ : Інститут стратегічних досліджень, 2017. 400 с. Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 Joint Communication to the European Parliament and the Council «Joint Framework on countering hybrid threats the European Union response» (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 Martti J. Kari (2019). Russian Strategic Culture in Cyberspace. Theory of Strategic Culture – A Tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats. University of Jyväskylä. 211 p. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. (2023). Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg [in English]. doi:10.2760/113791, JRC129019 The Temporary Protection Directive. URL: https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system/temporary-protection_en Balashov E., Bilokon M. Golovianko M. etc. (2023) Training methods in the context of hybrid threats. Харків. 84 с. DOI: https://doi.org/10.62067/978-617-8242-02-2
16	Specific equipment, hardware and software for the course	WARN-Hub (building 7, room 214), funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Art Management and Event Technologies Phone: (044)280 4554 Page: https://nakkkim.edu.ua/instituti/instituti-institut-praktichnoji-kulturologiji-ta-art-menedzhmentu/kafedra-art-menedzhmentu-ta-ivent-tekhnologij

		Email: artmanager@dakkkim.edu.ua
18	Teacher(s) – syllabus designer(s)	Associate professor of the Department of Cultural studies and intercultural communication Reva Tetiana, PhD in Political Studies, associate professor treva@dakkkim.edu.ua

2.11 KhNU (P10): Master Programme on Public Policy and Administration under Conditions of Hybrid Threats

№	Name of the field	Course Title: **Hybrid Threats and Comprehensive Security**
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	281 Public Administration
3	Type and the title of the study programme	Master Programme on Public Administration
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 18 hours, seminars/practical classes – 30 hours, independent work of students – 102 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year / 1 semester
10	Course objectives	Providing a set of systematized theoretical knowledge and mastering practical skills and skills for international and Ukrainian experience in combating hybrid threats in the context of comprehensive security.
11	Learning outcomes	● Understand the complex nature, complexity, logic and patterns of hybrid threats. ● Detect, identify, classify hybrid threats and respond effectively to them in cross-sectoral interaction. ● Analyze problems caused by hybrid threats, and make effective management decisions to overcome such problems. ● Identify and classify hybrid threats, evaluate the effectiveness of existing forms and methods of public administration in terms of combating hybrid threats. ● Develop effective management decisions in the context of hybrid threats within their professional competence.
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI".

		Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing. Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, infrastructure domains. Module 4. Tools of hybrid threat activity: system of tools of hybrid influencing; operations against infrastructure; cyber espionage and cyber operations, electronic operations, economic, military / paramilitary, sociocultural, tools in public administration, legal, intelligence-diplomatic, information-analytical, media tools. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. Module 6. Basics of protection: history of the issue and basic approaches to countering to hybrid threats; comprehensive security concept; the comprehensive resilience ecosystem (CORE) model; self assessment; countering; detecting (monitoring vs discovery) of hybrid threats; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats.
13	Students performance evaluation	Individual work: Report (in printed or electronic version) on the implementation of individual educational and practical tasks (15), presentation (15) - report, presentation, report and discussion. All tasks are completed, conclusions are made, the material is presented logically and meaningfully, complete answers to questions and good discussion skills - 30 points There are insignificant shortcomings in the performance of tasks and presentations - 20 points Certain tasks are not completed or there are significant errors, shortcomings in the conclusions, incomplete answers, or no presentation of the task - 10 points. The presentation does not correspond to the structure of tasks, only some aspects of the tasks are presented, insufficient level of mastery of the material - 5 points. Activity in the classroom (30). Survey on the tasks of independent work. Incomplete answer / remark is estimated by a decrease of 50%. Final test (40): 40 questions of 1 point each, covering all course modules.
14	Quality assurance of the educational process	Course policy on adherence to the principles of academic integrity. Strict adherence to the principles of academic integrity in accordance with the Regulations on the system of prevention and detection of academic plagiarism in scientific and educational works

		of employees and graduates of Kharkiv National University named after VN Karazin (put into effect by order of the rector № 0501-1/173 from 14.05.2015, https://www.univer.kharkov.ua/docs/antiplagiat_nakaz_polozhennya.pdf).
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE, https://www.hybridcoe.fi/ Website of EU East StratCom Task Force (ESTF), https://euvsdisinfo.eu/ Glossary of hybrid threats, https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 Benjamin Miller. The Concept of Security: Should it be Redefined? Journal of Strategic Studies, 2001. Vol. 24:2, P. 13-42. Stephen M. Walt. The Renaissance of Security Studies. International Studies Quarterly, Vol. 35, No. 2 (Jun., 1991), P. 211-239. URL: http://users.metu.edu.tr/utuba/Walt%20Renais.pdf. Hoffman F.G. Incognito Hybrid Threats: Avoiding the Alliance’s Trident. From the North Atlantic to the South China Sea. Nomos Verlagsgesellschaft mbH & Co. KG, 2021. URL: https://www.nomos-elibrary.de/10.5771/9783748921011-69/incognito-hybrid-threats-avoiding-the-alliance-s-trident. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899. Monaghan Sean (Ed.), Patrick Cullen, and Njord Wegge. 2019. MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. 94 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.
16	Specific equipment, hardware and software for the course	Specialized educational and research laboratory at the Department of Digital Technologies and e-Government of the Institute of Public Administration of KhNU. V.N. Karazina is a part of the educational process on counteracting hybrid threats, and also is a part of the trans sectoral academic environment countering hybrid threats. In 2021, the European Union under the Erasmus + KA2 program, the project "WARN: Academic Response to Hybrid Threats" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) funded the purchase of laboratory equipment worth more than 250 thousand UAH.

17	Department	Department of Public Policy Department of Law, National Security and European Integration https://ipa.karazin.ua/?page_id=11726&lang=en

18	Teacher(s) – syllabus designer(s)	Dr. Viacheslav Dziundziuk, Doctor of Public Administration, Professor, Head of the Department of Public Policy;
		Dr. Larysa Velychko, Doctor of Laws, Professor, Head of the Department of Law, National Security and European Integration;
		Alexander Kotukov, PhD in Sociology, Associate Professor of the Department of Public Policy;
		Mykhailo Bilokon, PhD in Public Administration, Associate Professor of the Department of Law, National Security and European Integration.

2.12 DSPU (P11): Master Programme on Teacher Training (Secondary school) History, Psychology

№	Name of the field	Course Title: Hybrid Threats and Comprehensive Security
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	014 Teacher training (Secondary school)
3	Type and the title of the study programme	Master Programme on Teacher training (Secondary school) History, Psychology
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	*5*
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 24 hours, seminars classes – 20 hours, practical classes – 10 hours, independent work of students – 96 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	Provide the knowledge and skills needed to understand, analyze and respond to hybrid threats in professional activities and societal life
11	Learning outcomes	● To implement in professional activities effective psychological and pedagogical strategies of human existence in society in the globalized socio-cultural environment and hybrid threats; ● To understand the complex nature, complexity, logic and patterns of hybrid threats, critically evaluate socio-political, economic, cultural events and phenomena; ● To identify, classify hybrid threats and respond to them effectively in intersectional cooperation; ● To act in a prudent way in a new situation, to implement effective strategies for human existence in society in the globalized socio-cultural environment and hybrid threats; ● To organize and implement educational activities for various categories of the population in the field of pedagogy, psychology, history, in particular on the detection and response to hybrid threats.
12	Course annotation (content)	Module 1. Asymmetry, hybrid threats and security: new security landscape and decision making; hybrid threats - history, definitions, essential features; PMESII spectrum; "4 + 1 + AI". Module 2. Conceptual model. The Landscape of Hybrid Threats: background, elements and structure of the model; state and non-state actors, their use in hybrid influencing.

		Module 3. The domains of malicious actions: critical functions and vulnerabilities; information, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political, infrastructure domains. Module 4. Tools of hybrid threat activity: system of tools of hybrid influencing (zagal characteristic). Social divisions in the Ukrainian society as a factor of hybrid threats. Module 5. Dynamics of hybrid threats: the role of different types of activities in the landscape of hybrid threats; phases of hybrid threats, hybrid activities. The hybrid nature of the current russian-Ukrainian war. Module 6. Basics of protection: history of the issue and basic approaches to countering to hybrid threats; comprehensive security concept (based on the Finnish model example); self assessment; countering; detecting (monitoring vs discovery) of hybrid threats; deterring; responding; principles of constructing the mechanisms for protection against hybrid threats.
13	Students performance evaluation	Assessment of students' knowledge of the discipline "Hybrid Threats and Comprehensive Security" is carried out by conducting control activities, which include current, final modular, final semester control. The level of academic achievement of students is assessed on a 100-point scale. The total amount of points consists of the points for checkpoints and module tests, which are conducted in practical classes, as well as the points received by the students in the exam
14	Quality assurance of the educational process	The course policy is based on the policy of the Horlivka Institute for Foreign Languages of Donbas State Pedagogical University. The result of preparation for a lesson should be a meaningful mastery of the topic material, namely: confirmation of theoretical material by examples from historical sources, knowledge of basic definitions, ability to present certain material, prepare a presentation of their own research, comment on other students' answers, supplement them, find mistakes (inaccuracies, shortcomings) and provide a correct answer, work in a team. The students' answer should show signs of independence in the performance of tasks, the absence of recurrence and plagiarism. Students must adhere to educational ethics, respect the participants in the learning process, be balanced, attentive and adhere to discipline and time parameters of the educational process.

15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/, Website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p. Sweijs, T., & Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. Hybrid threats: A comprehensive resilience ecosystem (2023). Aho A., Alonso Villota M., Giannopoulos G., Jungwirth R., Lebrun M., Savolainen J., Smith H., Willkomm E. URL: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ President of Estonia Alar Karis lecture at JYU, Jyvaskyla, Finland: Our strength is a path to peace, weakness breeds more war. 13 February 2024. URL: https://www.jyu.fi/en/news/president-alar-karis-on-martti-ahtisaari-lecture-our-strength-is-a-path-to-peace-weakness-breeds
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory for hybrid threats research is a participant in the intersectional environment for countering hybrid threats WARN (room 402). In 2021, the Lab was equipped with powerful computer hardware totally for almost 894 thousand UAH, funded by the grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) – destroyed in Bakhmut in 2023. In 2022, the institution received additional equipment for the organization of online education in the amount of almost 70 thousand UAH, funded by the grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Domestic and foreign history, room 304 (educational building)- http://forlan.org.ua/?page_id=49
18	Teacher(s) – syllabus designer(s)	Dokashenko Galyna, Doctor of History, Professor g.dokashenko@forlan.org.ua Dokashenko Viktor, Doctor of History, Professor v.dokashenko@forlan.org.ua

3 The New Courses for Each Project Master's Programme

3.1 NURE (P5): Analyzing and Countering Hybrid Threats in Business Management / Analysis and Countermeasures Against Hybrid Threats in Business Management

№	Name of the field	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	073 Management
3	Type and the title of the study programme	Master Programme on Financial and Economic Security Management
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 30 hours, seminars/practical classes – 20 hours, consultations – 10 hours, independent work of students – 90 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	Provide the knowledge and skills for hybrid threats prevention, hybrid campaigns identification and effective response in the domain of financial and economic security.
11	Learning outcomes	● To consider critically, to select and to use the necessary scientific, methodological and analytical tools for management under unpredictable conditions; ● To design effective systems for management of organizations; ● To have the skills of decision making, justification and implementation of management decisions within unpredictable conditions taking into account the requirements of the current legislation, ethical aspect and social responsibility; ● To detect, identify, classify hybrid threats and to be capable to respond to them effectively in trans-sectoral collaboration.
12	Course annotation (content)	Module I. Hybrid threats as a challenge to the business environment Topic 1. The impact of hybrid threats on socio-economic activity. Topic 2. Analysis of business management vulnerabilities in the context of hybrid threats. Module II. Analysis of the new role of business in the the contemporary security landscape Topic 3. The financial and economic sector as an object and tool of hybrid threats. Topic 4. Business resilience in the context of hybrid threats

		Module III. Mechanisms for counteracting hybrid threats in management Topic 5. Organization of financial and economic security in the context of hybrid threats Topic 6. Mechanisms of detecting and countering hybrid threats in the financial and economic security system
13	Students performance evaluation	Accumulating grades for the course: ● workshops (4 practical classes) – 10 points, ● Exploring the threatening differences between E-Democracy and E-Dictatorship (2 practical classes + independent work of students) – 20 points, ● strategic games "Analysis of hybrid influences in conflict studies" (2 practical classes + independent work of students) – 15 points, ● master class "Protection of business and business environment in conditions of hybrid threats" (2 practical classes + independent work of students) – 15 points ● exam – 20 points. Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	The policy of academic integrity among applicants at NURE provides advice on the requirements for implementing written works, emphasizing the principles of independence, correct use of information from other sources and avoidance of plagiarism, as well as rules for describing sources and citations. The content of the discipline is updated at the end of the previous semester at the initiative of the leading lecturer, considering educational and scientific interests of students. The content of the educational component is reviewed and updated annually, considering the results of a survey of stakeholders, discussed at meetings of the department and approved by the head of the support group of the specialty. The leading lecturer determines what modern practices and scientific achievements should be used in the educational process.
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/ Website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Aho A., Midões C., Šnore A. (2020) Hybrid threats in the financial system: Hybrid CoE Working Paper 8. - Helsinki, Finland: Hybrid CoE. Business community and hybrid threats: Report of Pasi Eronen Foundation for Defense of Democracies. Helsinki, 2018.

		Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023. 124 p. doi:10.2760/37899 Harjanne A., Muilu E., Pääkkönen J., Smith H. (2018) Helsinki in the era of hybrid threats – Hybrid influencing and the city. – Helsinki, Finland: Hybrid CoE. Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. - Swedish Defence University. ISBN 978-91-86137-73-1
16	Specific equipment, hardware and software for the course	The specialized educational FESM laboratory is a component of the interfaculty NURE Hub on countering hybrid threats, and also is a part of the trans sectoral academic environment countering hybrid threats. In 2021, FESM Lab was equipped with powerful computer hardware totally for more than 350 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Economic Cybernetics and Management of Economic Security, d_eces@nure.ua https://eces.nure.ua/
18	Teacher(s) – syllabus designer(s)	Dr. Svitlana Gryshko, PhD, svitlala.gryshko@nure.ua

3.2 NURE (P5): Hybrid Threats and Artificial Intelligence

№	Name of the field	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	122 Computer science
3	Type and the title of the study programme	Master Programme on Systems of Artificial Intelligence
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	*5*
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 30 hours, seminars/practical classes – 20 hours, consultations – 10 hours, independent work of students – 90 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year/2 semester
10	Course objectives	Provide the knowledge and skills for hybrid threats prevention, hybrid campaigns identification and effective response in the domain of artificial intelligence.
11	Learning outcomes	● To identify the concepts, algorithms and data structures needed to describe the domain of development or research; to perform decomposition of a given problem in order to apply known methods and technologies for its solving. ● To choose the appropriate means for development or research (e.g., development environment, programming language, software, and software packages) that allow finding the correct and effective solution. ● To apply the principles, techniques and tools of development or research used in the corresponding research and development domains; to create prototypes of software to ensure its compliance with design requirements; to perform software testing and static analysis to check that software addresses the task of development or research. ● To use artificial intelligence technologies for the development of decision-making systems and intelligent information systems to counter hybrid threats ● To apply ethical principles to the creation of artificial intelligence technologies ● To apply intelligent security technologies to protect vulnerable methods of artificial intelligence, e.g., deep learning, from cyber threats.

12	Course annotation (content)	Module 1. Introduction into the changing landscape of the global security Topic 1. Navigating the modern AI landscape. LLMs, transformers, their strengths and vulnerabilities. Topic 2. The impact of AI on hybrid warfare: cyber-enhanced hybrid threats (disruptive use of AI, expansion of the role of cyber during crises, dependency between society and technology). Module 2. Artificial Intelligence security Topic 1. Introduction into design and development of secure software. Security Concepts: Vulnerabilities, Threats, and Attacks. Software Security Foundations. Topic 2. Security of intelligent software. Resilience and robustness of AI models training and operation. Topic 3. Adversarial machine learning: adversarial attacks (types, definitions, consequences, countermeasures. Deep learning and security; attacks on computer vision. Topic 4. Using AI for cyber-security: attribution of attacks; detection of malicious activity. Game theory for security. Module 4. Artificial decision making and problem solving in adversarial environments. Topic 1. Game theory for decision-making in adversarial settings. Topic 2. Intelligence analysis; assessment of competing hypotheses. Module 5. Information management in hybrid warfare Topic 1. Information retrieval; disinformation; cryptography; information verification. Topic 2. Fighting disinformation with AI.
13	Students performance evaluation	Accumulating grades for the course: ● workshops (3 practical sessions) – 30 points, ● master class (1 practical session on fact checking) – 10 points, ● adversarial games (1 practical class: training generative adversarial networks) – 20 points, ● exam – 40 points. Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Academic integrity is fundamental for the educational process. The principles of academic integrity are described in the Regulations on fight against academic plagiarism in NURE and the Regulations on the organization of the educational process in NURE, p. 5.8. Evaluation of students performance is a tool to control the quality and to measure the achievement of the intended

		learning outcomes. Grades are based upon in-class (online) participation, learning activities, and assignments. The point values associated with each activity are delineated in the student evaluation section of this document. The criteria used in grading each assignment are discussed in class and are specified and provided in written form at the beginning of the course. Grades are assigned on the basis of accumulated points. All practical and lab works are implemented in groups in class. The presence of a student in class is a prerequisite for obtaining the maximal grade. The absence implies a 20% score reduction; the absence and the completion of the task after the deadline implies a 30% reduction of the grade. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/, Web-site of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 Kurakin, A., Goodfellow, I., & Bengio, S. (2016). Adversarial machine learning at scale. arXiv preprint arXiv:1611.01236. Ivan, C., Chiru, I., & Arcos, R. (2023). Hybrid Security Threats and the Information Domain: Concepts and Definitions. In *Routledge Handbook of Disinformation and National Security* (pp. 9-19). Routledge. Thiele, R. (2020). Hybrid CoE Working Paper 6. Artificial Intelligence – A key enabler of hybrid warfare. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf Jerbi, S., Gyurik, C., Marshall, S. C., Molteni, R., & Dunjko, V. (2024). Shadows of quantum machine learning. *Nature Communications*, *15*(1), 5676. Stenzel, G., Zorn, M., Altmann, P., Mansky, M. B., Kölle, M., & Gabor, T. (2024, July). Self-Replicating Prompts for Large Language Models: Towards Artificial Culture. In *ALIFE 2024: Proceedings of the 2024 Artificial Life Conference*. MIT Press.

16	Specific equipment, hardware and software for the course	The specialized educational AI laboratory is a component of the interfaculty NURE Hub on countering hybrid threats, and also is a part of the trans sectoral academic environment countering hybrid threats. In 2021, AI Lab was equipped with powerful computer hardware totally for more than 420 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Artificial Intelligence (AI), http://ai.nure.ua, d_ai@nure.ua
18	Teacher(s) – syllabus designer(s)	Dr. Mariia Golovianko, PhD, mariia.golovianko@nure.ua

3.3 UCU (P6): Recognizing and Countering Hybrid Threats in Public Administration

№	Name of the field	Content, comments
1.	Level of higher education	Second cycle (master`s degree)
2.	Subject area	281 Public administration
3.	Type and the title of the study programme	Master Programme on Public Administration
4.	Type of the course	Elective
5.	Language of instruction	Ukrainian
6.	Number of ECTS credits	5
7.	Structure of the course (distribution of the types and the hours of the study)	Lectures – 30 hours, practical classes – 20 hours, consultation – 10 hours, independent work of students – 90 hours
8.	Form of the final evaluation	Pass/fail grading
9.	Year of study/semester when the course is delivered	Year 1, Semester 2
10.	Course objectives	• learn to distinguish and analyze different types of hybrid threats; • master models of hybrid actions in the fight against information and cyber threats; • to acquire skills in the development and implementation of communication activities in the field of hybrid threats; • possession (understanding) of technologies and capabilities for countering and strengthening resistance to hybrid threats; • critical assessment of the international experience of countering hybrid threats and substantiation of the expediency of its implementation on a national scale; • learn to analyze the opponent's strategies based on the wargaming approach in the educational process.
11.	Learning outcomes	Know the basic principles of national security and be able to warn and neutralize challenges and threats to the national interests of Ukraine within the limits of their professional competence. Carry out effective management of innovations, resources, risks, projects, changes, quality, apply modern models, approaches and technologies, international experience in the design and reorganization of management and general organizational structures. To be able to communicate effectively, argue one's position, and use modern information and communication technologies in the field of public management and administration on the basis of social responsibility and

		legal and ethical norms. Develop well-founded management decisions taking into account issues of European and Euro-Atlantic integration, take into account goals, existing legislative, time and resource limitations, and evaluate political, social, economic and environmental consequences of decision options. Demonstrate an understanding of the complex nature, complexity, logic, and patterns of hybrid threats. Identify and classify hybrid threats and effectively respond to them in cross-industry interaction. Have the knowledge, technology and capabilities to counter and enhance resilience to hybrid threats.
12.	Course annotation (content)	Module 1. Theoretical bases of studying hybrid threats (+ legal aspects) Module 2. Features of hybrid influence in the public sector Module 3. Methods for detecting hybrid effects Module 4. Information dimension of hybrid threats Module 5. Economic dimension of hybrid threats Module 6. Cyber dimension of hybrid threats Module 7. Countering hybrid threats and developing resilience. Module 8. EU and NATO initiatives to counter hybrid threats Module 9. The experience of the Eastern and European Union countries in building state capabilities to counter hybrid threats Module 10. Ukrainian experience: combating hybrid threats and resilience.
13.	Students performance evaluation	Accumulation of points in the discipline: workshops (3 practical tasks) - 30 points, team projects (2 team tasks) - 40 points, mini-research (1 on a self-selected topic) - 20 points wargaming (1 matrix game) - 10 points Maximum number of points - 100 (60 and more - credited, 59 and less - not credited)
14.	Quality assurance of the educational process	The course will apply UCU's policies on academic integrity and plagiarism prevention, which can be found at this link: https://s3.eu-central-1.amazonaws.com/ucu.edu.ua/wp-content/uploads/2024/02/2024.-Polozhennya-pro-zapobigannya-akademichnomu-plagiatu-ta-inshym-vydam-porushen.pdf
15.	Recommended or required	Glossary of hybrid threats https://warn-

	reading and other learning resources/tools	erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 Hybrid CoE key themes for 2023 https://www.hybridcoe.fi/wp-content/uploads/2023/01/Hybrid-CoE-key-themes-for-2023.pdf Henrik Praks (2024) Hybrid CoE Working Paper 32: Russia’s hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage URL: https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf Harjanne A., Muilu E., Pääkkönen J., Smith H. (2018) Helsinki in the era of hybrid threats – Hybrid influencing and the city. – Helsinki, Finland: Hybrid CoE. URL:https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf Hybrid CoE Trend Report 4: Trends in the Contemporary Information Environment (2020) Hybrid CoE Trend Report 4: Trends in the Contemporary Information Environment - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats Hybrid CoE Trend Report 6: The future of cyberspace and hybrid threats (2021)Hybrid CoE Trend Report 6: The future of cyberspace and hybrid threats - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019. https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf
16.	Specific equipment, hardware and software for the course	UCU University Newsroom is part of an inter-program Hub for countering hybrid threats, as well as a member of the trans-sectoral environment for countering hybrid threats WARN. In 2021, the newsroom received computer equipment totalling more than UAH 750,000, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid

		Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). University computer laboratories with appropriate software, UCU library fund
17.	Department	School of Public Management (spm@ucu.edu.ua)
18.	Teacher(s) – syllabus designer(s)	Myroslava Chekh, Oksana Vasylytsia miroslava@ucu.edu.ua, vasylytsya@ucu.edu.ua

3.4 UCU (P6): Hybrid Threats in Media Communications

№	Name of the field	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	061 Journalism
3	Type and the title of the study programme	Master Programme on Media Communications
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 30 hours Seminars/practical classes – 30 hours Independent work of students – 90 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	Year 2, Semester 2
10	Course objectives	Provide the knowledge and skills needed to understand, analyze and respond to hybrid threats in professional activities and societal life
11	Learning outcomes	Understand the complex nature, complexity, logic and patterns of hybrid threats. Ensure public stability and uninterrupted professional activity in conditions of hybrid threats Be able to respond to fakes and manipulations and narratives that are manifestations of hybrid threats. Identify narratives that are manifestations of hybrid threats and plan their professional activities, including the creation of information campaigns taking into account these features Identify and analyze the main features, tools, forms and methods of hybrid narratives. Be able to use OSINT tools to counter hybrid threats. Build communication strategies and information campaigns based on hybrid threats. Analyze the nature and features of hybrid threats in media and digital communications: Students will be able to explain the concept and manifestations of hybrid threats, particularly in the context of media communications, digital platforms, and social networks, while understanding their impact on political and economic life. Identify and counteract manipulation and fake messages: Students will learn to detect manipulation, disinformation, and hybrid narratives using digital tools, applying techniques like Open Source Intelligence (OSINT) to identify and combat hybrid threats in both traditional and digital spaces. Assess vulnerabilities and future risks in the digital landscape:

		Students will evaluate the vulnerabilities of critical infrastructure, individuals, businesses, and the state to hybrid threats, considering the impact of emerging technologies such as artificial intelligence and virtual reality, while proposing strategies to mitigate future risks.
12	Course annotation (content)	Module 1. Introduction. The concept of hybrid threats. The hybrid threats' manifestations and features. Hybrid threats in media communications. Media and information contexts of hybrid threats Module 2. The global context of hybrid threats, global practices to combat them. Hybrid threats in the political and economic life of Ukraine: historical aspect and current challenges Module 3. Hybrid threats and fake messages. Manipulation, narratives. Their identification and counteraction. Digital tools for identifying and combating hybrid threats Module 4. Hybrid influences: main features, forms, methods of implementation. Tools and scenarios of hybrid influences Module 5. Hybrid threats in the digital space. Social networks as platforms for the dissemination of hybrid narratives. Problems of modern online services and search engines in the context of hybrid influences Module 6. World practice of combating hybrid threats in the digital space. Countering hybrid threats in the digital space: tools and methods. OSINT and OSINT tools in the identification of hybrid threats Module 9. Hybrid threats and digital security: digital vulnerabilities for individuals, businesses and the state. The concept of critical infrastructure and vulnerabilities of its objects. IT development and hybrid threats. Future risks in the field of new technologies - artificial intelligence, virtual and augmented reality, social platforms, meta-universes
13	Students performance evaluation	The grade for the course is the sum of the grades for the current completed tasks, modular tests and the final test task. Scoring is based on a 100-point system in accordance with the ECTS system, which is translated into a 4-point (national) scale in accordance with the "Regulations on the procedure for assessing student knowledge in the credit-module organization of the UCU educational process." The control measure is a test. СЗ (100) = М (10) + П (60) + З (30) М – assessment for modular control, П – the sum of points for current tasks, З – assessment for the test Modular control methods: closed tests. The grade for the module is 10 points out of 100

		Current tasks: OSINT work; identification of hybrid threats; essays on a selected topic
14	Quality assurance of the educational process	The course will apply UCU's policies on academic integrity and plagiarism prevention, which can be found at this link: https://bit.ly/3IXhZlz
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/, website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats, https://warn-erasmus.eu/ua/glossary/ Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p.Sweijs, T., & Zilincik, S. (2019). Cross-Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.
16	Specific equipment, hardware and software for the course	UCU University Newsroom is part of an inter-program Hub for countering hybrid threats, as well as a member of the trans-sectoral environment for countering hybrid threats WARN. In 2021, the newsroom received computer equipment totalling more than UAH 750,000, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). University computer laboratories with appropriate software, UCU library fund.
17	Department	School of Journalism and Communication, http://sjc.ucu.edu.ua/
18	Teacher(s) – syllabus designer(s)	Nadiya Balovsyak, Associate Professor of Media Communications balovsyak@ucu.edu.ua

3.5 SUIT (P7): Recognizing and Countering Hybrid Threats in Transport and Logistics

№	Field name	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	073 Management
3	Type and the title of the study programme	Master Programme on Organization Management and Administration
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	4
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 20 hours, seminars/practical classes – 24 hours, independent work of students – 76 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1st year / 2nd semester
10	Course objectives	To develop a system of knowledge and skills necessary to perform organizational, analytical and advisory functions to recognize and counter hybrid threats in transportation and logistics.
11	Learning outcomes	● To demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats. ● To detect, identify, classify hybrid threats and to be capable to respond to them effectively in transsectoral collaboration.
12	Course annotation (content)	Module 1. Conceptual framework for ensuring national resilience in Ukraine Module 2. Foreign experience in ensuring resilience in the security sector Module 3. The problem of ensuring the national resilience of Ukraine, taking into account the negative impact of hybrid threats on the development of critical infrastructure Module 4. Ensuring the resilience of the transport and logistics system of Ukraine in the context of countering hybrid threats Module 5. Management of transport infrastructure development in the system of economic security of Ukraine
13	Students performance evaluation	Type of work (*maximum points)*: current control - *max 80, exam - max 20.* Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Adherence to the principles of academic integrity is carried out in accordance with the Code of Academic Integrity of the State University of Infrastructure and Technologies, the Regulations on the system of academic integrity in the State University of Infrastructure and Technologies and the

		principles of academic integrity. organization of the educational process at the State University of Infrastructure and Technologies, p.4.9. The tool of control measures is a rating assessment of students. Each point is awarded for a specific achievement, a list of which is published at the beginning of the course. During the semester, students "gain" a certain number of points for the results of their work. All practical and lab works are implemented in groups in class. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students
15	Recommended or required reading and other learning resources/tools	Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с. URL: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf NATO’S RESILIENCE CONCEPT AND UKRAINE. URL: http://prismua.org/en/nato_ukraine/ Giannopoulos G., Jungwirth R., Hadjisavvas C., et.al., Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EN, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/58406, JRC133083. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC133083 Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ: НАН України, 2022. 552 с. URL: https://ipiend.gov.ua/publication/natsionalna-stijkist-ukrainy-stratehiia-vidpovidi-na-vyklyky-ta-vyperedzhennia-hibrydnykh-zahroz/ Шемаєв В.В. Управління розвитком транспортної інфраструктури в системі економічної безпеки держави:. дис. ... д-ра екон. наук : 21.04.01; Нац. ін-т стратег. дослідж. Київ, 2018. 494 с.
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory is a component of the Faculty of Management and Technology of the State University of Infrastructure and Technologies, a member of the trans-sectoral environment for combating hybrid threats WARN.

		In 2021, the laboratory received powerful computer equipment totaling more than 736 thousand UAH, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE -JP)
17	Department	Department of Management and Public Administration, room 608.
18	Teacher(s) – syllabus designer(s)	Karpenko Oksana, Doctor of Sciences in Economics, Professor, Professor of the Department of Management and Public Administration karpo_2004@ukr.net Osypova Yevheniia, Candidate of Sciences in Economics, Associate Professor, Associate Professor of the Department of Management and Public Administration, layretta@ukr.net

3.6 SUIT (P7): Information security and Hybrid Threats

№	Field name	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	121 "Software Engineering"
3	Type and the title of the study program	Master Program on Software Engineering
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	3
7	Structure of the course (distribution of the types and the hours of the study)	Lectures - 20 hours, practical classes - 10 hours, independent work - 60 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1st year / 2nd semester
10	Course objectives	to acquire the necessary practical skills to develop and study prototypes of information security subsystems under the influence of hydride threats, which are the implementation of effective approaches and algorithms to create a comprehensive system to protect information from unauthorized access.
11	Learning outcomes	● PH12. Make effective organizational and managerial decisions in conditions of uncertainty and changing requirements, compare alternatives, and change risks. ● PH19. Identify and classify hybrid threats and respond effectively to them in intersectoral interaction.
12	Course annotation (content)	Topic 1. Problems of information security in computer systems. Topic 2. Analysis of information security threats. Topic 3. Ensuring information security based on a risk-oriented approach. Topic 4. Analysis and assessment of information security risks. Topic 5. Identification and evaluation of the value of assets as key risk factors. Topic 6. Analysis of the main and hybrid threats and vulnerabilities of information systems. Topic 7. Information risk management model. Topic 8. An integrated approach to the design of information security systems based on resilience as a key safety property.
13	Students performance evaluation	Type of work (*maximum points)*: current control - *max 60, exam - max 40.* Maximum – 100 points (60 and more – pass, 59 and less – fail)

14	Quality assurance of the educational process	Adherence to the principles of academic integrity is carried out in accordance with the Code of Academic Integrity of the State University of Infrastructure and Technologies, the Regulations on the system of academic integrity in the State University of Infrastructure and Technologies and the principles of academic integrity. organization of the educational process at the State University of Infrastructure and Technologies, p.4.9. The tool of control measures is a rating assessment of students. Each point is awarded for a specific achievement, a list of which is published at the beginning of the course. During the semester, students "gain" a certain number of points for the results of their work. All practical and lab works are implemented in groups in class. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students
15	Recommended or required reading and other learning resources/tools	Vilmer, J.-B. Jeangène, Escorcia, A., Guillaume, M., Herrera, J. (2018) Information Manipulation: A Challenge for Our Democracies, the report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces. France, Paris. 208 p. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf Курбан О. В. Основи сучасної національної інформаційної безпеки України. *Вісн. ХДАК*. 2017. Вип. 50. С. 55-62. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуал. пробл. політики.* 2016. Вип. 58. С. 66-76. Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. Swedish Defence University. ISBN 978-91-86137-73-1. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThre-ats.pdf
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory is a component of the Faculty of Management and Technology of the State University of Infrastructure and Technology, a member of the trans-sectoral environment for combating hybrid threats WARN. In 2021, the laboratory received powerful computer equipment totaling more than 736 thousand UAH, funded by a grant from the Erasmus + project "Academic Counteraction

		to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE -JP)
17	Department	Department of Information Technology and Design, aud. 601a
18	Teacher(s) – syllabus designer(s)	Mukhin Vadym, Doctor of Technical Sciences, Professor, Professor of the Department Information Technology and design v_mukhin@i.ua

3.7 SUIT (P7): Recognizing and Countering Hybrid Threats in Transport and Logistics (additionally)

№	Name of the field	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	051 Economics
3	Type and the title of the study programme	Master Programme on Economics
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	3
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 20 hours, seminars/practical classes – 10 hours, independent work of students – 60 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1st year / 2nd semester
10	Course objectives	To develop a system of knowledge and skills necessary to perform organizational, analytical and advisory functions to recognize and counter hybrid threats in transportation and logistics.
11	Learning outcomes	● To formulate, analyze, and synthesize solutions to scientific and practical problems. ● To communicate fluently on professional and scientific issues in the state and foreign languages orally and in writing. ● To evaluate the results of their own work, demonstrate leadership skills, and the ability to manage staff and work in a team. ● To make effective decisions under uncertain conditions and requirements that require the use of new approaches, methods, and tools of socio-economic research. ● To develop scenarios and strategies for the development of socio-economic systems. ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in transsectoral collaboration.
12	Course annotation (content)	Module 1. The conceptual framework for ensuring national resilience in Ukraine Module 2. Foreign experience in ensuring resilience in the security sector

		Module 3. The problem of ensuring the national resilience of Ukraine, taking into account the negative impact of hybrid threats on the development of critical infrastructure Module 4. Ensuring the resilience of the transport and logistics system of Ukraine in the context of countering hybrid threats Module 5. Management of transport infrastructure development in the system of economic security of Ukraine
13	Students performance evaluation	Type of work (*maximum points)*: current control - *max 80, exam* - *max 20.* Maximum – 100 points (60 and more – pass, 59 and less – fail)
14	Quality assurance of the educational process	Adherence to the principles of academic integrity is carried out in accordance with the Code of Academic Integrity of the State University of Infrastructure and Technologies, the Regulations on the system of academic integrity in the State University of Infrastructure and Technologies and the principles of academic integrity. organization of the educational process at the State University of Infrastructure and Technologies, p.4.9. The tool of control measures is a rating assessment of students. Each point is awarded for a specific achievement, a list of which is published at the beginning of the course. During the semester, students "gain" a certain number of points for the results of their work. All practical and lab works are implemented in groups in class. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students
15	Recommended or required reading and other learning resources/tools	Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с. URL: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf NATO'S RESILIENCE CONCEPT AND UKRAINE. URL: http://prismua.org/en/nato_ukraine/ Giannopoulos G., Jungwirth R., Hadjisavvas C., et.al., Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EN, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/58406, JRC133083. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC133083

		Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ : НАН України, 2022. 552 с. URL: https://ipiend.gov.ua/publication/natsionalna-stijkist-ukrainy-stratehiia-vidpovidi-na-vyklyky-ta-vyperedzhennia-hibrydnykh-zahroz/ Шемаєв В.В. Управління розвитком транспортної інфраструктури в системі економічної безпеки держави:. дис. ... д-ра екон. наук : 21.04.01; Нац. ін-т стратег. дослідж. Київ, 2018. 494 с.
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory is a component of the Faculty of Management and Technology of the State University of Infrastructure and Technologies, a member of the trans-sectoral environment for combating hybrid threats WARN. In 2021, the laboratory received powerful computer equipment totalling more than 736 thousand UAH, funded by a grant from the Erasmus + project "Academic Counteraction to Hybrid Threats - WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE -JP)
17	Department	Department of Management and Public Administration, room 608.
18	Teacher(s) – syllabus designer(s)	Karpenko Oksana, Doctor of Sciences in Economics, Professor, Professor of the Department of Management and Public Administration karpo_2004@ukr.net Osypova Yevheniia, Candidate of Sciences in Economics, Associate Professor, Associate Professor of the Department of Management and Public Administration, layretta@ukr.net

3.8 NUOA (P8): Public Discourse as a Component of Information Wars

№	Name of the field	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	25 Military sciences, national security; 256 National security (for certain areas of support and types of activity)
3	Type and the title of the study programme	Master Programme on National security (for certain areas of support and types of activity)
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 16 hours, seminars/practical classes – 14 hours, independent work of students – 120 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	1 year, 1 semester
10	Course objectives	Provide the knowledge and skills needed to understand the information policy of the state in the context of hybrid warfare, as well as a methodology for analyzing and responding to hybrid threats in the information sphere.
11	Learning outcomes	● To demonstrate an understanding of the complex nature, complexity, logic, and patterns of hybrid threats; ● To effectively use the normative legal framework for the activities of the subjects of the organization of state and non-state (media) information policy in the context of hybrid aggression. ● To use effectively the essential characteristics of public discourse in the context of the threat of a hybrid war; a mechanism for counteracting information and psychological operations of the enemy; acquisition of a set of skills and abilities to analyze practical problems of organizing information and psychological operations in professional activities; ● To ensure social stability and uninterrupted professional activity in the context of hybrid threats. ● To demonstrate an understanding of the complexity, difficulty, logic and patterns of hybrid threats; ● To detect, identify, and classify hybrid threats and to be capable of responding to them effectively in trans-sectoral collaboration. ● To develop strategic decisions based on scenario analysis using normal-form and hybrid military simulations.

12	Course annotation (content)	Module 1. Public discourse: the problem of theoretical identification. Module 2. Hybrid warfare as a discursive construct. Module 3. Hybrid warfare in the educational dimension. Module 4. Practice and theory of mass communication. Module 5. Features of information warfare in the media. Module 6. Strategies and technologies of wars of the information age. Methods of normal-form games and hybrid military simulations. Module 7. Counterpropaganda Discourse in a Hybrid War.
13	Students performance evaluation	Accumulating grades for the course: ● 7 practical classes – 70 points, ● Scientific essay – 20 points, ● Test – 20 points. Maximum – 100 points (61 and more – pass, 60 and less – fail)
14	Quality assurance of the educational process	Procedures for adherence to the principles of academic integrity are regulated by the Regulations on Ensuring the Quality of Educational Activities and the Quality of Higher Education in NUOA and the principles of academic integrity set forth in the NUOA Education Regulations and the Code of Academic Integrity The instrument of monitoring is the rating assessment of students. Each point is awarded for a specific achievement, a list of which will be published at the beginning of the course. During the semester, students receive points for their performance in each lesson. The presence of a student in each class is a prerequisite for obtaining a 100% grade. At the end of the course, anonymous feedback regarding the usefulness of the proposed material and the complexity of the work are obtained from the students.
15	Recommended or required reading and other learning resources/tools	Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Webster F. Theories of the Information Society. SecondEdition. London, NewYork. - 2002. Institute for Propaganda Analysis. Propaganda, How to Recognize It and Deal With It. Hassell Street Press, 2021. 88 p. Jon Roozenbeek. Propaganda and Ideology in the Russian–Ukrainian War (Contemporary Social Issues Series). Cambridge University Press; New edition. 2024. 234 p. Jeffrey Appleget, Robert Burks. The Craft of Wargaming: A Detailed Planning Guide for Defense Planners and Analysts. Naval Institute Press. 2020. 376 p.

16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory “Laboratory for Research on Hybrid Threats to National Security” (LRHTNS) is a component of the Educational and Scientific Institute of International Relations and National Security of NUOA and also is a part of the trans-sectoral academic environment countering hybrid threats. In 2021, the educational and research laboratory LRHTNS was equipped with powerful computer hardware totally for more than 350 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Political Sciences and National Security, new campus *Tel.* +38 (03654) 22949, https://www.oa.edu.ua/ua/departments/mizhn/pim_polit/ kafedra.politologii@oa.edu.ua
18	Teacher(s) – syllabus designer(s)	Dr., Sanzharevskyi Oleh Ivanovych, PhD, oleh.sanzharevskyi@oa.edu.ua Mozol Mykhailo Leonidovych mykhailo.mozol@oa.edu.ua

3.9 NUOA (P8): Recognizing and Countering Hybrid Threats in Political Sciences

№	Name of the field	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	052 Political Sciences
3	Type and the title of the study program	Master Programme on Political Sciences
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 16 hours, seminars/practical classes – 14 hours, independent work of students – 120 hours
8	Form of the final evaluation	Pass/fail grading
9	Year of study/semester when the course is delivered	1 year/1 semester
10	Course objectives	Training of highly qualified specialists possessing modern knowledge, skills and competencies necessary to understand the role and place of hybrid threats in the context of modern politics, political process and national security of the state, which will enable them to formulate and solve practical problems, conduct research and effectively execute professional activities.
11	Learning outcomes	● to understand the basic concepts and theoretical and methodological approaches in modern political science; ● to understand the theoretical and practical aspects of politics and political process; ● to understand the essence, role, and place of ensuring security as one of the basic functions of the state and state policy; ● to demonstrate an understanding of the complex nature, complexity, logic, and patterns of hybrid threats; ● to use the experience of NATO member states and other leading foreign countries in protecting the national security of the state in the context of hybrid threats; ● to ensure social stability and uninterrupted professional activity in the context of hybrid threats; ● to detect, identify, and classify hybrid threats and to be capable of responding to them effectively in transsectoral collaboration. ● to conduct a detailed analysis of information operations and cyberattacks, identifying their goals, methods, and potential impact on political processes.

12	Course annotation (content)	Module 1. Basic concepts and modern theoretical and methodological approaches in modern political science. Module 2. Theoretical and practical aspects of the concepts of politics and political process. Module 3. Ensuring national security as one of the basic functions of the state and public policy. Module 4. Hybrid warfare: origins, evolution, modern forms. Module 5. The essence and key parameters of modern hybrid threats. Module 6. Internal and external aspects of detection and counteraction to hybrid threats. Cyberspace and political stability. Module 7. International cooperation in detecting and counteracting hybrid threats.
13	Students performance evaluation	Accumulating grades for the course: ● 7 practical classes – 70 points, ● Scientific essay – 20 points, ● Test – 20 points. Maximum – 100 points (61 and more – pass, 60 and less – fail)
14	Quality assurance of the educational process	Procedures for adherence to the principles of academic integrity are regulated by the Regulations on Ensuring the Quality of Educational Activities and the Quality of Higher Education in NUOA and the principles of academic integrity set forth in the NUOA Education Regulations and the Code of Academic Integrity The instrument of control activities is the rating assessment of students. Each point is awarded for a specific achievement, a list of which will be published at the beginning of the course. During the semester, students receive points for their performance in each lesson. The presence of a student in each class is a prerequisite for obtaining a 100% grade. At the end of the course, anonymous feedbacks regarding the usefulness of the proposed material and the complexity of the work are obtained from the students.
15	Recommended or required reading and other learning resources/tools	Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Стратегічне планування: вирішення проблем національної безпеки. Монографія / В. П. Горбулін, А. Б. Качинський. – К. : НІСД, 2010. – 288 с. Aho A., Alonso Villota M., Giannopoulos G., Jungwirth R., Lebrun M., Savolainen J., Smith H., Willkomm E. Hybrid threats: A comprehensive resilience ecosystem. 2023. 120 p.

17		Andrej Poleščuk, Veronika Krátka Špalková. Hybrid CoE Research Report 10: Preventing election interference: Selected best practices and recommendations. 2023. 63 p. Sebastian Bay. Hybrid CoE Research Report 12: Countering hybrid threats to elections: From updating legislation to establishing collaboration networks. 2024. 39 p.
16	Specific equipment, hardware, and software for the course	The specialized educational and research laboratory “Laboratory for Research on Hybrid Threats to National Security” (LRHTNS) is a component of the Educational and Scientific Institute of International Relations and National Security of NUOA and also is a part of the trans-sectoral academic environment countering hybrid threats. In 2021, the educational and research laboratory LRHTNS was equipped with powerful computer hardware totally for more than 350 thousand UAH, funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Political Sciences and National Security, new campus *Tel.* +38 (03654) 22949, https://www.oa.edu.ua/ua/departments/mizhn/pim_polit/ kafedra.politologii@oa.edu.ua
18	Teacher(s) – syllabus designer(s)	Dr. Zhovtenko Taras Hryhorovych, PhD, Taras.Zhovtenko@oa.edu.ua Dr., Prof. Atamanenko Alla Yevhenivna alla.atamanenko@oa.edu.ua

3.10 NAMSCA (P9): Cultural Practices as an Instrument for Countering Hybrid Threats in the Real and Virtual Environment

№	Field name	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	028 Management of Sociocultural Activities
3	Type and the title of the study program	Master Programme on Cross-cultural Management
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 20 hours Seminars – 8 hours Practical lessons – 12 hours Individual work – 100 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1st year / 2nd semester
10	Course objectives	● To get knowledge about modern functional cultural practices, their definition, and their importance in overcoming hybrid challenges; ● To gain the skills of using methods, and techniques of creating cultural practices, which are used to overcome hybrid threats; ● To be able to detect, prevent, and respond professionally to manifestations of cultural trauma, genocide, and anomie.
11	Learning outcomes	LO 3. To be able to collect and integrate evidence of their own research position, substantiate the results of sociocultural practices, and to present and tell opinion on the results of research and innovation. LO 8. To use the «4-c model» to solve problems and make decisions, conduct negotiations and scientific discussions in the field of sociocultural management. LO 9. To present and discuss the results of scientific and applied research, sociocultural strategies, and projects in the state and foreign languages; LO 13. To understand and apply in practice theoretical and methodological knowledge on the theory of the sociocultural systems; LO 14. The ability to create a perspective cross-cultural environment with adaptive socio-cultural practices and a system of responding to hybrid challenges.

		LO 15. To ability to work in the conditions of the transformation processes, caused by hybrid threats.
12	Course annotation (content)	Content module 1: THEORETICAL CONCEPTIONS OF CULTURAL PRACTICES AND HYBRID THREATS 1.1. Competence relevance of the discipline (2 hours) 1.2. Cultural practices and hybrid threats: operationalization of concepts and conceptualization of the phenomena (2 hours) Content module 2: AXIOLOGICAL APPROACH TO THE CULTURAL AND PRACTICAL TOOLS FOR COUNTERING HYBRID THREATS 2.1. Value orientations of cultural practices and their role in the hybrid threats resistance (2 hours) 2.2. Cultural rights and freedoms in the optics of hybrid threats (2 hours) Content module 3: CULTURAL TRAUMA, SHOCK AND GENOCIDE: IDENTIFYING AND OVERCOMING PRACTICES 3.1. Cultural trauma and shock: practical instruments to identify and the strategies of the resistance (2 hours) 3.2. Cultural genocide: global and local characteristics (2 hours) Content module 4: CULTURAL DIPLOMACY AS SOFT POWER: TOOLS AND PRACTICES 4.1. Cultural diplomacy tools in the system of overcoming hybrid threats (2 hours) 4.2. The practices of cultural diplomacy in the global-local dimension of the hybrid challenges (2 hours) Content module 5: THE AGENTS OF CULTURE: PRACTICES OF SUSTAINABILITY, CULTURE, ACCULTURATION IN REAL AND VIRTUAL ENVIRONMENTS 5.1. The Agents of cultures, mission, and goals in the system of hybrid challenges overcoming (2 hours) 5.2. The practices of culture sustainability in the real and virtual environment (2 hours)
13	Students performance evaluation	Forms of Control: 1. Evaluation of student's work at practical lessons –21 points (from 0 to 3 points for every task). 2. Evaluation of student's work at seminars –21 points (from 0 to 3 points for every task). 3. Individual work – 28 points (from 0 to 2 points for every task). 4. Exam – 30 points (the project work). Scale of Evaluation: According to the national differential scale – «Excellent», «Good», «Satisfied», «Unsatisfied».

		According to the ECATS scale: A 90-100, B 82-89, C 74-81, D 64-73, E 60-63, FX 35-59, F 1-34.
14	Quality assurance of the educational process	All participants of the educational process follow the policy of academic integrity and contribute to functioning effective system of the academic plagiarism prevention and detection.
15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/, Website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Kopiyevska, O. Creative Discourses of Educational Practices: Student Youth of Arts and Culture Professions// Youth Voice Journal, 2021. ISBN (ONLINE): 978-1-911634-21-8 Elwell, F.L. (2013) Sociocultural systems: Principles of structure and change. Athabasca University Press, 2013. https://www.aupress.ca/app/uploads/120219_99Z_Elwell_2013-Sociocultural_Systems.pdf Frese M. (2015) Cultural Practices, Norms, and Values. Journal of Cross-Cultural Psychology. Volume: 46 issue: 10, P. 1327-1330. https://doi.org/10.1177/0022022115600267 Manterys A. (2018). Cultural Practices and Social Relations. // Individuals and their social contexts. Warsaw. Institute of Political Studies of the Polish Academy of Sciences (pp.113-150) Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023 https://publications.jrc.ec.europa.eu/repository/handle/JRC129019
16	Specific equipment, hardware, and software for the course	WARN-Hub (building 7, room 214), funded by a grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Department of Art Management and Event Technologies Phone: (044)280 4554 Page: https://nakkkim.edu.ua/instituti/instituti-institut-praktichnoji-kulturologiji-ta-art-menedzhmentu/kafedra-art-menedzhmentu-ta-ivent-tekhnologij Email: artmanager@dakkkim.edu.ua
18	Teacher(s) – syllabus designer(s)	Professor of the Department of Cultural studies and intercultural communication Kopiievska Olha, Doctor in Cultural studies, professor okopievska@gmail.com

3.11 KhKNU (P10): Recognizing and Countering Hybrid Threats in Public Administration

№	Field name	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	281 Public administration
3	Type and the title of the study program	Master Programme on Public policy and administration under conditions of hybrid threats
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 20 hours, seminars/practical classes – 30 hours, independent work of students – 100 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	2 year / 3 semester
10	Course objectives	Providing a set of systematic theoretical knowledge and mastering practical skills and abilities to recognize and combat hybrid threats in public administration in modern conditions within its competence.
11	Learning outcomes	● Understand the complex nature, complexity, logic, and patterns of hybrid threats. ● Detect, identify, and classify hybrid threats and respond effectively to them in cross-sectoral interaction. ● Develop public policy measures and analyze them taking into account existing and potential hybrid threats. ● Know the features of the public administration system in the context of globalization. ● Carry out their responsibilities with regard to national security, using legal and information and communication mechanisms to counter hybrid threats.
12	Course annotation (content)	Topic 1. Formation and implementation of public policy taking into account hybrid threats Topic 2. Public policy analysis: the impact of hybrid threats Topic 3. Globalization and its impact on modern social relations Topic 4. The impact of globalization on public administration Topic 5. International and national security systems in conditions of hybrid threats Topic 6. Features of international conflicts and hybrid aggression Topic 7. International law in the context of hybridization of international conflicts

14		Topic 8. Institutional and Legal counteraction to Hybrid Threats at the National Level Topic 9. The problem of information security of the state in the context of modern threats Topic 10. Psychological influence as a factor in the threat to information security in Ukraine Topic 11. Developing Resilience in the Face of Hybrid Threats
13	Students performance evaluation	Individual work: Report (in printed or electronic version) on the implementation of individual educational and practical tasks (20), presentation (20) - report, presentation, report, and discussion. All tasks are completed, conclusions are made, the material is presented logically and meaningfully, complete answers to questions and good discussion skills - 40 points There are insignificant shortcomings in the performance of tasks and presentations - 30 points Certain tasks are not completed or there are significant errors, shortcomings in the conclusions, incomplete answers, or no presentation of the task - 20 points. The presentation does not correspond to the structure of tasks; only some aspects of the tasks are presented, and there is an insufficient level of mastery of the material - 10 points. Activity in the classroom (30). Survey on the tasks of independent work. An incomplete answer / remark is estimated by a decrease of 50%. Final test (30): 30 questions of 1 point each, covering all course topics.
14	Quality assurance of the educational process	Course policy on adherence to the principles of academic integrity. Strict adherence to the principles of academic integrity in accordance with the Regulations on the system of prevention and detection of academic plagiarism in scientific and educational works of employees and graduates of V. N. Karazin Kharkiv National University (put into effect by order of the rector № 0501-1/173 from 14.05.2015, https://www.univer.kharkov.ua/docs/antiplagiat_nakaz_polozhennya.pdf).

15	Recommended or required reading and other learning resources/tools	Website of Hybrid CoE https://www.hybridcoe.fi/, Website of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Wigell, M., Scholvin, S., & Aaltola, M. (Eds.). (2018). Geo-Economics and Power Politics in the 21st Century: The Revival of Economic Statecraft. Routledge. Linkov, I., & Trump, B. D. (2019). The science and practice of resilience. Springer International Publishing.
16	Specific equipment, hardware and software for the course	Specialized educational and research laboratory at the Department of Digital Technologies and e-Government of the Institute of Public Administration of KhNU. V.N. Karazina is a part of the educational process of counteracting hybrid threats and also is a part of the trans-sectoral academic environment countering hybrid threats. In 2021, the European Union under the Erasmus + KA2 program, the project "WARN: Academic Response to Hybrid Threats" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) funded the purchase of laboratory equipment worth more than 250 thousand UAH.
17	Department	Department of Public Policy Department of Law, National Security, and European Integration 61001, Ukraine, Kharkiv, 75 Heroyv Kharkova Ave. +38 (050) 591-11-22, +38 (098) 112-21-00 ipa@karazin.ua

18	Teacher(s) – syllabus designer(s)	Dr. Viacheslav Dziundziuk, Doctor of Public Administration, Professor, Head of Public Policy Department (topics – 1, 2);
		Dr. Larysa Velychko, Doctor of Laws, Professor, Head of Law, National Security and European Integration Department (topics – 7, 8);
		Dr. Alexander Orlov, Doctor of Public Administration, Professor, Professor of Public Policy Department (topics – 9, 10);
		Dr. Alexander Kotukov, PhD in Sociology, Associate Professor of Public Policy of Public Policy Department (topics – 3, 4);
		Dr. Mykhailo Bilokon, PhD in Public Administration, Associate Professor of Law, National Security and European Integration Department (topics – 5, 6).

3.12 DSPU (P11): History and Hybrid Threats

№	Field name	Content, comments
1	Level of higher education	Second cycle (master`s degree)
2	Subject area	014 Teacher Training (Secondary school)
3	Type and the title of the study programme	Master Programme on Teacher Training (Secondary school) History, Psychology
4	Type of the course	Compulsory
5	Language of instruction	Ukrainian
6	Number of ECTS credits	5
7	Structure of the course (distribution of the types and the hours of the study)	Lectures – 20 hours, seminars classes – 20 hours, practical classes – 14 hours, independent work of students – 96 hours
8	Form of the final evaluation	Exam
9	Year of study/semester when the course is delivered	1 year/2 semester
10	Course objectives	The purpose of the course is to acquaint students with the main directions and methods of using history as a tool of manipulation and hybrid threats and identify ways to debunk historical myths and opportunities to resist attempts to instrumentalize history in professional activities and public life.
11	Learning outcomes	The ability to study effectively different historical sources, to distinguish specifics in approaches to solving historical problems in different scientific fields and schools, to comprehend critically the latest achievements of historical science in order to identify hybrid threats. The skill to analyze the phenomena and processes of world and domestic history, taking into account modern theories of social development and possible hybrid threats. The skill to determine the information potential of specific historical sources in solving the problem of the objectivity of historical material presentation to identify hybrid threats; The ability to understand the world model, nature, causal patterns of social development and the links of different cultures; to respect different cultures, religions, peoples, and human rights; to preserve peace and tolerant existence, to respond effectively to the manifestations of hybrid threats The ability to navigate freely in information and Internet sources, use library and archival funds, be critical of the information received, be able to classify hybrid threats, have a computer and information culture. The ability to work effectively in a professional and / or scientific group, adhere to ethical standards of professional activity and academic integrity.

12	Course annotation (content)	Module 1. The phenomenon of instrumentalization of history. History as a narrative about the past and a lesson for the present. Factors of representation of the past in scientific research, journalism, and media. Basic historical concepts of modernity. The concept of "Russian world" as an ideological platform for instrumentalizing the history of Ukraine in the hybrid war. Module 2. The main directions of domestic and foreign distortion. History of Ukraine: the history of Ukrainian statehood; the history of the formation of the Ukrainian ethnos; the falsification of the Holodomor-genocide of the Ukrainian people; the history of Ukrainian culture, its role, and its place in the general treasury of civilization. World History: the formation of the Russian Empire; the October coup of 1917 in the history of the former "national outskirts"; World War II and the postwar world order; "soft justification of Stalin's repressions" as a component of Stalinist policy. IPSO - a component of the hybrid Russian-Ukrainian war Module 3. The ways to recognize and counter hybrid threats in history. The concept of alternative history. A historical source as a basis for studying the historical process. The ways of formation and development of critical thinking on historical material.
13	Students performance evaluation	Assessment of students' knowledge of the discipline is carried out by conducting control activities, which include current, final modular, final semester control. The level of academic achievement of students is assessed on a 100-point scale. The current control includes students' oral answers to theoretical questions of seminars, test tasks, team projects, independent work, solving game situations. The final control (exam) objectively confirms students' level of education, to determine the degree of their skills and abilities at the end of the semester. The general assessment consists of the sum of points for checkpoints and test work of the content module, gained during the semester and the points received in the exam.
14	Quality assurance of the educational process	The course policy is based on the policy of the Horlivka Institute for Foreign Languages of Donbas State Pedagogical University. The result of preparation for a lesson should be a meaningful mastery of the topic material, namely: confirmation of theoretical material by examples from historical sources, knowledge of basic definitions, ability to present certain material, prepare a presentation of their own research, comment on other students' answers, supplement them, find

		mistakes (inaccuracies, shortcomings) and provide a correct answer, work in a team. The students' answer should show signs of independence in the performance of tasks, the absence of recurrence and plagiarism. Students must adhere to educational ethics, respect the participants in the learning process, be balanced, attentive and adhere to discipline and time parameters of the educational process.
15	Recommended or required reading and other learning resources/tools	Web-site of Hybrid CoE https://www.hybridcoe.fi/, Web-site of EU East StratCom Task Force (ESTF) https://euvsdisinfo.eu/ Glossary of hybrid threats https://warn-erasmus.eu/ua/glossary/ Grigas, A. (2016). Beyond Crimea: the new Russian empire. Yale University Press. – 352 p. ISBN 0300220766 http://maxima-library.org/knigi/genre/b/382587?format=read Simons, G. (2015). Perception of Russia's soft power and influence in the Baltic States. Public Relations Review, 41(1), 1-13. https://doi.org/10.1016/j.pubrev.2014.10.019 Hosaka, Sanshiro. 2019. “Welcome to Surkov’s Theater: Russian Political Technology in the Donbas War.” Nationalities Papers 47(5) Hosaka, Sanshiro. 2020. “Repeating History: Soviet Offensive Counterintelligence Active Measures.” International Journal of Intelligence and CounterIntelligence, 1 – 30 Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985
16	Specific equipment, hardware and software for the course	The specialized educational and research laboratory for hybrid threats research is a participant in the intersectional environment for countering hybrid threats WARN (room 402). In 2021, the Lab was equipped with powerful computer hardware totally for almost 894 thousand UAH, funded by the grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)– destroyed in Bakhmut in 2023. In 2022, the institution received additional equipment for the organization of online education in the amount of almost 70 thousand UAH, funded by the grant of the Erasmus+ project "Academic Response to Hybrid Threats – WARN" (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)
17	Department	Domestic and foreign history, room 304 (educational building)- http://forlan.org.ua/?page_id=3

18	Teacher(s) – syllabus designer(s)	Dokashenko Galyna, Doctor of History, Professor, g.dokashenko@forlan.org.ua Dokashenko Viktor, Doctor of History, Professor v.dokashenko@forlan.org.ua