PROJECT
Considered at the meeting of the department on January 16, 2026, Protocol No. 9

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL TECHNICAL UNIVERSITY
"KHARKIV POLYTECHNIC INSTITUTE"

APPROVED
Rector of NTU "KhPI"
_____ Yevgen SOKOL
"____" _____ 2026

EDUCATIONAL AND PROFESSIONAL PROGRAM "CYBERSECURITY"

Second (Master's) level of higher education

in specialty **F5 – Cybersecurity and information protection**
fields of knowledge **F - Information technologies**
qualification **Master of cybersecurity and information protection**

APPROVED
ACADEMIC COUNCIL OF NTU
"Khpi"
Head of the academic council
_____/ Yevgen SOKOL
Protocol №. ___
From_____

Kharkiv 2026

LETTER OF AGREEMENT

Educational and professional program «Cybersecurity»

Level of higher education	Second (Master's) level
Branch of knowledge	F Information technologies
Specialty	F5 Cybersecurity and information protection
Qualification	Master of cybersecurity and information protection

APPROVED
The EPP workgroups for the specialty «Cybersecurity and information protection»
Guarantor of the educational program

_____ Olga KOROL

Protocol №. ___

From_____2026

RECOMMENDED
Methodical council of NTU "KhPI"
Deputy chairman of the methodical council

_____ Ruslan MYGUSHCHENKO

Protocol №. ___

From_____2026

AGREED
Head of the Department of Cybersecurity

_____ Sergii YEVSEIEV

Protocol №. ___

From_____2026

AGREED
Director of the Educational and Scientific Institute of Computer Science and Information Technology

_____ Mykhailo HODLEVSKYI

«____»_____2026

AGREED
Higher education
(member of the EPP workgroup)
№ group KH-M1125

_____ Pavlo POZHYDAIEV

«____»_____2026

APPROVED AND GRANTED
By order of the rector of the National Technical University "Kharkiv Polytechnic Institute" from _____2026 No._____.

REVIEWERS:

Productive remarks and feedback on the project of the educational-professional program received from:

1. OPIRSKY Ivan, Doctor of Technical Sciences, Professor, Head of the Department of Information Protection of the Institute of Computer Technology, Automation and Metrology of the National University "Lviv Polytechnic".
2. KOVTUN Vladyslav, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.
3. GOLOVASHYCH Serhii, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.
4. VOLOSHCHUK Olena, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.
5. SHAPOVAL Olga, Executive Director of Kharkiv Cluster of Information Technology

Reviews

PREFACE

Corresponds to the Standard of Higher Education of the second (Master's) level in specialty F5 "Cybersecurity and information protection", which was approved by the order of the Ministry of Education and Science of Ukraine dated 18.03.2021 No. 332.

Developed by the working group of the EPP "Cybersecurity"
Educational and Scientific Institute of Computer Sciences and Information Technologies of the National Technical University "Kharkiv Polytechnic Institute" consisting of:

Guarantor of the educational and professional program
KOROL Olga, candidate of technical sciences, associate professor, associate professor of the cybersecurity department.

Members of the workgroup EPP:

1. YEVSEIEV Sergii, doctor of technical sciences, professor, head of the cybersecurity department.
2. POHASII Serhii, doctor of technical sciences, associate professor, professor of the cybersecurity department.
3. MILEVSKYI Stanislav, doctor of technical sciences, associate professor, professor of the cybersecurity department
4. POZHYDAIEV Pavlo, student, group KH- M1125.

1. PROFILE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM BY SPECIALTY F5 – CYBERSECURITY AND INFORMATION PROTECTION

1 - General information	
Higher education institution and structural unit	National Technical University "Kharkiv Polytechnic Institute", Educational and Scientific Institute of Computer Sciences and Information Technologies department of cybersecurity
The degree of higher education and the title of the qualification in the original language	The degree of higher education – Master Branch of knowledge – F Information technologies Specialty – F5 Cybersecurity and information protection Educational qualification – master of cybersecurity and information protection.
Professional qualification	There is no
Form of study	Institutional (full -time), remote)
The official name of the educational program	Cybersecurity
Names of specializations (subject specialties)	There is no
Type of diploma single, common (double) in the presence and volume of educational program	Master's Diploma, Single, 90 ECTS credits, study period 1 year 4 months
Availability of accreditation	National Higher Education Quality Agency. Accreditation certificate educational program No. 6112 Valid up to 01.07.2029
Cycle/level	second (master's) level of higher education; NRK of Ukraine – level 7, FQ-EHEA – second cycle, EQF LLL – level 7
Prerequisites	The presence of higher education first (bachelor) level.
Language of teaching	Ukrainian, English
The term of validity of the educational program	According to the validity of the certificate Reviewed annually
Link to the permanent posting of the description of the educational program	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-magistr/
2 - The purpose of the educational and professional program	
Training specialists capable of solving research and/or innovative tasks in the field of information and/or cybersecurity, use and introduce technologies and use the means of protection in the safety systems of the contour of business processes.	
3 – Characteristics of the educational and professional program	
Subject area (field of knowledge, specialty,	**Field of knowledge:** F "Information technologies" **Specialty:** F5 "Cybersecurity and information protection"

specialization or subject specialty (if any)	**Object of study:** -modern processes of research, analysis, creation and maintenance of information systems and technologies, other business operational processes on the objects of information activity and critical infrastructures of the field of information security and/or cybersecurity; -information systems (information, communication, information and telecommunication, automated) and technologies; - infrastructure of information activity and critical infrastructure; - systems and complexes of creation, processing, transmission, storage, destruction, protection and display of data (information flows); - information resources of different classes (including state information resources); -software and software (means) of cyber defense; - information safety and/or cybersecurity management systems; - technologies, methods, models and information security and/or cybersecurity. **Training goals:** training of specialists who can solve research and/or innovative problems in the field of information and/or cybersecurity. **Theoretical content of the subject area:** theoretical foundations of science -intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision -making, systematic analysis, complex systems, modeling and optimization of processes, theory of mathematical statistics, cryptographic and technical protection. **Methods , techniques and technologies :** methods, models, techniques and technologies of creation, processing, transmission, acceptance, destruction, protection, protection (cyber defense) of information resources in cyberspace, as well as methods and models of development and use of applied and specialized software for solving professional problems in the field of information security and/or cybersecurity. Technologies, methods and models of research, analysis, management and provision of business/operational processes with the use of a set of regulatory and organizational and technical methods and means of protection of information resources in cyberspace. **Tools and equipment :** tools, devices, network equipment and environment, applied and specialized software, automated

	systems and design complexes, modeling, operation, control, monitoring, processing, displaying and protection of data (information flows), as well as methods and models of risk theory and management of information resources in the study and supporting information security and/or cybersecurity objects.
Orientation of the educational program	Educational and professional. Professional training in cybersecurity and information protection.
The main focus of the educational program and specialization or subject specialty (if any)	An in-depth study of both external and inner audits to ensure the safety of business processes. Obtaining Cisco Academy Certificates contributes to increased competitiveness in the labor market, improving audit mechanisms and protection by peace methods. Keywords: cybersecurity, digital forensics, ethical hacking.
Features of the program	The peculiarities of the program are the formation of the skills of constructing complex information security systems for ensuring the safety of business processes on the basis of modern technologies and software applications, in the conditions of development of digital economy. Orientation to partnership with domestic and foreign educational and science institutions, private sector, scientists and practitioners, participation in international programs of joint diplomas. Ability to learn English.
4 – Eligibility of graduates to employment and academic rights of graduates	
Suitability for employment	Cybersecurity and information protection experts can work in accordance with the current version of the National Classifier of Ukraine: Classifier of Professions DK 003: 2010, namely: 2139.2 Security threats; 2139.2 Analyst of information protection systems and vulnerability assessment; 2139.2 Analyst for the safety of information and communication systems; 2139.2 Investigator (cybersecurity and information security); 2139.2 Digital forensic expert (cybersecurity and information security); 2139.2 Forensic examination expert (cybersecurity and information protection); 2139.2 Investigator of cybercrime.
Academic rights of graduates	Students who have been trained under this curriculum and received a master's degree have the right to receive education at the third (educational and scientific) level of higher education in the HUB of Ukraine and abroad in the field of

	knowledge "information technologies" or related. Acquisition of additional qualifications in the adult education system.
5 – Teaching and assessment	
Teaching and learning	The teaching process provides for the use of educational technologies such as: lectures, laboratory work, practical classes, small groups, presentations that develop communicative and leadership skills, independent work with literary sources.
Assessment	Rating system of evaluation. Current and final knowledge control (surveys, control and individual tasks, testing, etc.), tests and exams (oral and written), public protection of qualification or project. The evaluation system involves the use of the ECTS International System (with estimates A, B, C, D, E, F), the national system (with "excellent", "good", "satisfactory" and "unsatisfactory"), as well as a 100-point system of higher education institution with a established system of conformity.
6 – Software competencies	
Integral competence	The ability of a person to solve research and/or innovative problems in the field of information security and/or cybersecurity.
General competencies (GC) (defined by the standard of higher education of the specialty)	GC1. Ability to apply knowledge in practical situations. GC2. Ability to conduct research at an appropriate level. GC3. Ability to abstract thinking, analysis and synthesis. GC4.The ability to evaluate and ensure the quality of the work performed. GC5.The ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity).
Special competences (SC) (defined by the standard of higher education of the specialty)	SC1. The ability to reasonably apply, integrate, develop and improve modern information technologies, physical and mathematical models, as well as technologies for creating and using applied and specialized software to solve professional problems in the field of information security and/or cyber security. SC2. Ability to develop, implement and analyze regulatory documents, provisions, instructions and requirements of technical and organizational direction, as well as integrate, analyze and use the best global practices, standards in professional activities in the field of information security and/or cyber security. SC3. Ability to research, develop and support methods and means of information security and/or cyber security at objects of information activity and critical infrastructure.

	SC4. The ability to analyze, develop and support the information security and/or cyber security management system of the organization, to form information security strategy and policies taking into account domestic and international standards and requirements. SC5. The ability to research, system analysis and ensure the continuity of business/operational processes in order to determine the vulnerabilities of information systems and resources, analyze risks and determine the assessment of their impact in accordance with the established strategy and policy of information security and/or cyber security of the organization. SC6. The ability to analyze, control and provide a management system for access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization. SC7. The ability to research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general. SC8. The ability to research, develop, implement and support methods and means of cryptographic and technical protection of information at objects of information activity and critical infrastructure, in information systems, as well as the ability to evaluate the effectiveness of their use, according to the established strategy and policy of information security and/or cyber security of the organization. SC9. The ability to analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information security and/or cyber security of the organization as a whole. SC10. The ability to conduct scientific and pedagogical activities, plan training, monitor and support work with personnel, as well as make effective decisions on information security and/or cyber security.
7 - Learning outcomes	
The results of studies in the specialty (defined by the standard of higher education of the specialty)	LO1. Communicate freely in national and foreign languages, orally and in writing, to present and discuss the results of research and innovation, ensure business/operational processes and issues of professional activity in the field of information security and/or cyber security.

	LO2. Integrate fundamental and specialized knowledge to solve complex information security and/or cyber security challenges in broad or multidisciplinary contexts. LO3. Conduct research and/or innovation activities in the field of information security and/or cyber security, as well as in the field of technical and cryptographic protection of information in cyberspace. LO4. Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and/or cyber security. LO5. Critically consider the problems of information security and/or cyber security, including at the interdisciplinary and interdisciplinary level, in particular on the basis of understanding the new results of engineering and physical and mathematical sciences, as well as the development of technologies for creating and using specialized software. LO6. Analyze and evaluate the security of systems, complexes and means of cyber protection, technologies for creating and using specialized software. LO7. To justify the use, implement and analyze the best global standards, practices in order to solve complex problems of professional activity in the field of information security and/or cyber security. LO8. Research, develop and support systems and means of information security and/or cyber security at objects of information activity and critical infrastructure. LO9. Analyze, develop and support the organization's information security and/or cyber security management system based on the information security strategy and policy. LO10. Ensure the continuity of business/operational processes, as well as identify vulnerabilities of information systems and resources, analyze and assess risks for information security and/or cyber security of the organization. LO11. Analyze, control and ensure the effective functioning of the system for managing access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization. LO12. Research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general. LO13. Research, develop, implement and use methods and means of cryptographic and technical information protection of

	business/operational processes, as well as analyze and provide an assessment of the effectiveness of their use in information systems, objects of information activity and critical infrastructure. LO14. Analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information and/or cyber security as a whole. LO16. Make informed decisions on organizational and technical issues of information security and/or cyber security in complex and unpredictable conditions, including using modern methods and means of optimization, forecasting and decision-making. LO18. Plan training, as well as accompany and supervise work with personnel in the direction of information security and/or cyber security. LO19. Choose, analyze and develop appropriate typical analytical, calculation and experimental methods of cyber protection, develop, implement and support projects on information protection in cyberspace, innovative activities and protection of intellectual property. LO20. Set and solve complex applied engineering and scientific problems of information security and/or cyber security, taking into account the requirements of national and international standards and best practices. LO21. Use the methods of natural, physical and computer modeling to study processes related to information security and/or cyber security. LO22. Plan and carry out experimental and theoretical research, put forward and test hypotheses, choose suitable methods and tools for this, carry out statistical processing of data, evaluate the reliability of research results, argue conclusions. LO23. Justify the selection of software, equipment and tools, engineering technologies and processes, as well as their limitations in the field of information security and/or cyber security based on current knowledge in related fields, scientific, technical and reference literature and other available information.
8 – Resource support for program implementation	
Personnel support	Meets the personnel requirements for ensuring educational activities in the field of higher education in accordance with the current legislation of Ukraine (Resolution of the Cabinet of Ministers of Ukraine “On Approval of Licensing Conditions

	for Conducting Educational Activities of Education" of December 30, 2015 No. 1187, as amended by CMU Resolution No. 365 dated 24.03.2021. Annex 15-16). The composition of the working group of the educational program, the professorial teaching staff, which is involved in teaching disciplines in the specialty corresponds to the license conditions of conducting educational activities at the first (bachelor's) level of higher education. Teaching teachers, specialists and employees of IT companies, as well as foreign specialists are involved in teaching.
Material and technical support	Meets the technological requirements for the material and technical support of educational activities in the field of higher education in accordance with the current legislation of Ukraine (Resolution of the Cabinet of Ministers of Ukraine "On Approval of Licensing Conditions for Conducting Educational Activities of Education" of December 30, 2015, No. 1187, with changes made in accordance with CMU Resolution No. 365 dated 24.03.2021. Annex 17). Educational scientific production base in the form of: —The educational buildings, computer classes, combined by a local computer network with access to the Internet, multimedia equipment; specialized software,cyber polygon.
Informational and educational and methodological support	Meets the technological requirements for educational and methodological and information support of educational activities in the field of higher education in accordance with the current legislation of Ukraine (Resolution of the Cabinet of Ministers of Ukraine "On Approval of Licensing Conditions for Conducting Educational Activities of Education" of December 30, 2015, No. 1187, (as amended by CMU Resolution No. 365 of 24.03.2021. Annex 18). Information and educational-methodical support of the educational process is realized by the presence of the necessary educational and methodological literature: textbooks, manuals, methodological recommendations for practical classes, independent work, syabrose of educational components (https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-magistr/). Information resources are located in the funds of the scientific library of NTU "KPI", websites of graduation departments. The educational process uses LMS (Learning Management System).
9 – Academic mobility	
National credit mobility	On the basis of bilateral agreements between the National Technical University "Kharkiv Polytechnic Institute" and

	leading technical universities of Ukraine. It is regulated by the "Regulations on academic mobility of students, graduate students, doctoral students, scientific-pedagogical and researchers of NTU" KhPI ".
International credit mobility	On the basis of bilateral agreements. On the basis of bilateral agreements between the National Technical University "Kharkiv Polytechnic Institute" and higher educational establishments of foreign partner countries.
Education of foreign students of higher education	Preparation of foreign citizens is carried out in accordance with the requirements of the current legislation, provided that the previous educational level is recognized.

2. LIST OF EDUCATIONAL COMPONENTS OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM "CYBERSECURITY" AND THEIR LOGICAL SEQUENCE

2.2 List components of educational and professional program

Code n/a	Components of the educational and professional program	Credits ECTS	Final control form
1	2	3	4
1. Mandatory components of educational program			
1.1 General training			
GT 1	*Academic English*	*3*	*Exam*
GT 2	*Innovative entrepreneurship and management*	*3*	*Exam*
GT 3	*AI-Based Security*	*3*	*Exam*
GT 4	*Security of the Internet of Things and Services*	*4*	*Test*
1.2 Special (professional) training			
ST 1	*Fundamentals of scientific research*	*5*	*Exam*
ST 2	*Critical Infrastructure Security*	*5*	*Test*
ST 3	*Network and cloud security*	*5*	*Exam*
ST 4	*Protection of Distributed Services and Operating Platforms*	*4*	*Test*
ST 5	*Digital forensics*	*4*	*Test*
1.3 Practical training			
PT 1	*Pre-graduation internship*	*11*	*Test*
1.4 Preparation and defense of qualification work			
	Preparation and defense of qualification work	*11*	
General amount mandatory components		*58*	
2. Elective educational components			
2.1 Educational components of free choice of professional training of the general institutional catalog			
ECPT 1	*EC FC PT 1*	*4*	*Test*
ECPT 2	*EC FC PT 2*	*4*	*Test*
ECPT 3	*EC FC PT 3*	*4*	*Test*
ECPT 4	*EC FC PT 4*	*4*	*Test*
ECPT 5	*EC FC PT 5*	*4*	*Test*
ECPT 6	*EC FC PT 6*	*4*	*Test*
2.2 Educational components of free choice of general training			
ECGT 1	*EC FC GT 1*	*4*	*Test*
ECGT 2	*EC FC GT 2*	*4*	*Test*
Total amount for elective components:		***32***	
GENERAL SCOPE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM:		***90***	

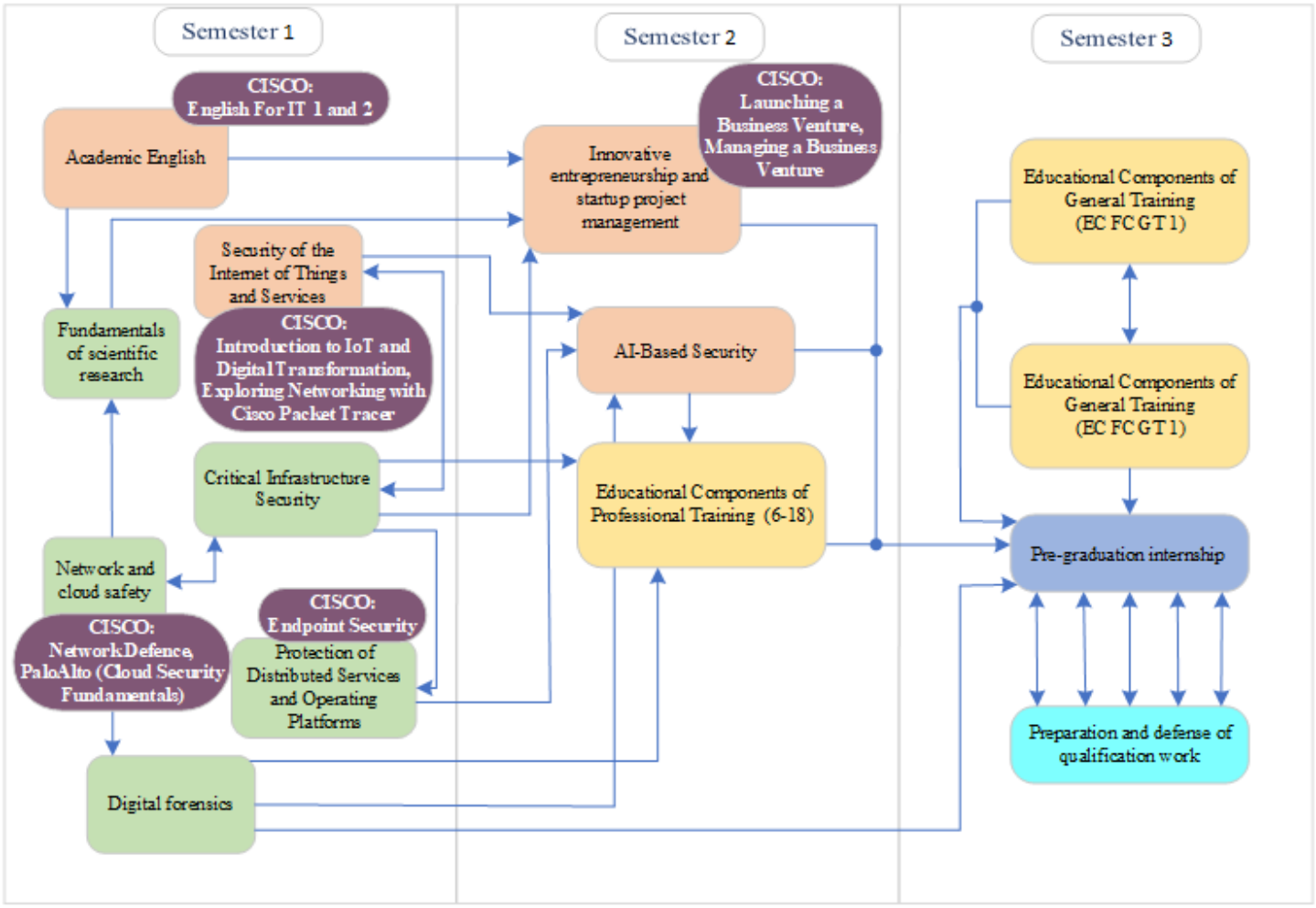
3. DISTRIBUTION CONTENT EDUCATIONAL AND PROFESSIONAL PROGRAMS BY IN GROUPS COMPONENTS AND CYCLES PREPARATION

No n/p	Cycle preparation	The amount of the applicant's educational loadhigher education (ECTS credits / %)		
		Mandatory components educational professional programs	Selective components educational professional programs	All in allterm teaching
1	General training	13 / 14,4	-	**13 / 14,4**
2	Special (professional) training	23 / 25,6	-	**23 / 25,6**
3	Practical training	11/12,2	-	**11/12,2**
4	Preparation and defense of qualification work	11/12,2	-	**11/12,2**
5	Optional educational components	-	32 / 35,6	**32 / 35,6**
Total for the entire term teaching		**58 / 64,4**	**58 / 64,4**	**32 / 35,6**

4. FORM CERTIFICATES EARNERS HIGHER EDUCATION

Forms of attestation of applicants of higher education	The certification is carried out in the form of public protection of qualification work.
Requirements for the unified state qualification exam	Qualification work should solve the complex problem of information security and/or cybersecurity and provide research and/or innovation. Qualification work should not contain academic plagiarism, fabrication, falsification. Qualification work should be posted on the official site (or in repository) of a higher education institution or its unit. The publication of restricted qualification works is carried out in accordance with the requirements of the legislation.

5. STRUCTURAL AND LOGICAL SCHEME



6. THE MATRIX OF COMPLIANCE OF THE COMPETENCES / LEARNING OUTCOMES DEFINED BY THE STANDARD WITH THE NQF DESCRIPTORS

Classification of competences according to NRC	**Knowledge** **Kn1** Specialized conceptual knowledge, including modern scientific achievements in the field of professional activity or field of knowledge and is the main one for original thinking and research, critical comprehension	**Skill** **Sk1** Specialized Skills/Skills of Problems Needed to Conduct Innovation Research and/or Pursuing Innovative Activity in order to develop new knowledge and procedures **Sk2** The ability to integrate knowledge and solve complex tasks in wide or mcultisciplinary contexts **Sk3** The ability to solve problems in new subscribers in the presence of incomplete or limited information taking into account aspects of social and ethical responsibility	**Communication** **C1** Clear and unambiguous communication of their own knowledge, conclusions and argumentation to specialists, in particular to persons studying	**Responsibility and autonomy** **AB1** Management of work or educational processes that are complex, unpredictable and require new strategic approaches **AB2** Responsibility for contribution to professional knowledge and practice and/or evaluation of the results of teams and teams **AB3** The ability to continue learning with a high degree of autonomy
GENERAL COMPETENCES				
GC1	Kn1,	Sk1, Sk3	C1	AB1, AB2
GC2	Kn1,	Sk1, Sk2, Sk3		AB2, AB3
GC3	Kn1	Sk2, Sk3		AB1
GC4	Kn1	Sk3		AB1, AB2
GC5	Kn1	Sk2	C1	AB1
SPECIAL (PROFESSIONAL) COMPETENCES				
SC1	Kn1	Sk2		AB2
SC2	Kn1,	Sk2		AB2
SC3	Kn1	Sk, Sk2, Sk3	C1	AB1, AB2
SC4	Kn1,	Sk, Sk2	C1	AB1, AB2
SC5	Kn1,	Sk1, Sk2	C1	AB1, AB2
SC6	Kn1	Sk1, Sk2	C1	AB1
SC7	Kn1	Sk1, Sk2	C1	AB1
SC8	Kn1	Sk1, Sk2	C1	AB1
SC9	Kn1	Sk1, Sk2	C1	AB1
SC10	Kn1	Sk1, Sk2, Sk3	C1	AB1, AB2

PROJECT
Considered at the meeting of the department on January 16, 2026, Protocol No. 9

7. CORRESPONDENCE MATRIX OF DEFINED LEARNING OUTCOMES, COMPETENCIES AND EDUCATIONAL COMPONENTS

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
LO 1	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1			GT1, GT2, GT4, PT3, PT4, T1									
LO 2		GT1, GT4, PT1, PT2, PT4, T1	GT1, PT1, PT2, T1			GT1, GT2, GT4, PT3, PT4, T1	PT1, PT2, T1	GT3, PT1, PT2, PT3, PT4, PT5, T1							
LO 3	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1					GT1, GT2, GT4, PT3, PT4, T1									
LO 4	GT1, GT2, GT3, GT4, PT1,	GT1, GT4, PT1, PT2, PT4,	GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1		GT1, GT2, GT4, PT3, PT4,	PT1, PT2, T1								

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	PT2, PT3, PT4, T1	T1				T1									
LO 5			GT1, PT1, PT2, T1		GT1, GT4, PT1, PT2, PT3, PT5, T1		PT1, PT2, T1								
LO 6	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1			GT4, PT1, PT2, PT4, T1		GT1, GT2, GT4, PT3, PT4, T1		GT3, PT1, PT2, PT3, PT4, PT5, T1		GT3, GT4, PT1, PT2, PT3, PT5, T1	GT2, T1	GT3, PT1, PT2, PT3, PT5, T1		GT4, PT1, PT2, PT3, PT4, T1	
LO 7	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1				PT1, PT2, T1								
LO 8	GT1, GT2, GT3, GT4, PT1,	GT1, GT4, PT1, PT2, PT4,		GT4, PT1, PT2, PT4, T1	GT1, GT4, PT1, PT2, PT3,			GT3, PT1, PT2, PT3, PT4,						GT4, PT1, PT2, PT3, PT4,	GT1, PT1, T1

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	PT2, PT3, PT4, T1	T1			PT5, T1			PT5, T1						T1	
LO 9	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1	GT1, GT4, PT1, PT2, PT4, T1	GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1					PT3, T1					GT4, ST1, PT2, PT3, PT4, T1	GT1, PT1, T1
LO 10	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1						GT3, GT4, PT1, PT2, PT3, PT5, T1				GT4, PT1, PT2, PT3, PT4, T1	
LO 11	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1							GT2, T1				GT1, PT1, T1
LO 12	GT1, GT2, GT3,		GT1, PT1, PT2,	GT4, PT1, PT2,					PT3, T1			GT3, PT1, PT2,			GT1, PT1, T1

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	GT4, PT1, PT2, PT3, PT4, T1		T1	PT4, T1								PT3, PT5, T1			
LO 13	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1									GT3, T1		GT1, PT1, T1
LO 14	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1					PT3, T1					GT4, PT1, PT2, PT3, PT4, T1	GT1, PT1, T1
LO 15				GT4, PT1, PT2, PT4, T1	GT1, GT4, PT1, PT2, PT3, PT5, T1										GT1, PT1, T1
LO 16	GT1, GT2, GT3,	GT1, GT4, PT1,	GT1, PT1, PT2,	GT4, PT1, PT2,				GT3, PT1, PT2,	PT3, T1	GT3, GT4, PT1,	GT2, T1	GT3, PT1, PT2,		GT4, PT1, PT2,	GT1, PT1, T1

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	GT4, PT1, PT2, PT3, PT4, T1	PT2, PT4, T1	T1	PT4, T1				PT3, PT4, PT5, T1		PT2, PT3, PT5, T1		PT3, PT5, T1		PT3, PT4, T1	
LO 17								GT3, PT1, PT2, PT3, PT4, PT5, T1							GT1, PT1, T1
LO 18	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1			GT4, PT1, PT2, PT4, T1	GT1, GT4, PT1, PT2, PT3, PT5, T1										GT1, ST1, T1
LO 19	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1			GT4, PT1, PT2, PT4, T1	GT1, GT4, PT1, PT2, PT3, PT5, T1	GT1, GT2, GT4, PT3, PT4, T1	PT1, PT2, T1	GT3, PT1, PT2, PT3, PT4, PT5, T1	PT3, T1		GT2, T1	GT3, PT1, PT2, PT3, PT5, T1	GT3, T1	GT4, PT1, PT2, PT3, PT4, T1	
LO 20	GT1, GT2, GT3,	GT1, GT4, PT1,	GT1, PT1, PT2,	GT4, PT1, PT2,	GT1, GT4, PT1,	GT1, GT2, GT4,		GT3, PT1, PT2,							

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	GT4, PT1, PT2, PT3, PT4, T1	PT2, PT4, PT, T1	T1	PT4, T1	PT2, PT3, PT5, T1	PT3, PT4, T1		PT3, PT4, PT5, T1							
LO 21	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1	GT1, GT4, PT1, PT2, PT4, T1	GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1		GT1, GT2, GT4, PT3, PT4, T1		GT3, PT1, PT2, PT3, PT4, PT5, T1		GT3, GT4, ST1, ST2, ST3, ST5, T1		GT3, ST1, ST2, ST3, ST5, T1	GT3, T1		
LO 22		GT1, GT4, ST1, ST2, ST4, T1	GT1, ST1, ST2, T1	GT4, ST1, ST2, ST4, T1		GT1, GT2, GT4, ST3, ST4, T1		GT3, PT1, PT2, PT3, PT4, PT5, T1							
LO 23	GT1, GT2, GT3, GT4, PT1, PT2, PT3, PT4, T1		GT1, PT1, PT2, T1	GT4, PT1, PT2, PT4, T1		GT1, GT2, GT4, PT3, PT4, T1	PT1, PT2, T1	GT3, PT1, PT2, PT3, PT4, PT5, T1			GT2, T1	GT3, PT1, PT2, PT3, PT5, T1	GT3, T1	GT4, PT1, PT2, PT3, PT4, T1	

8. THE RESULTS OF DISCUSSING THE EDUCATIONAL PROGRAM

Stakeholders	Remarks / Recommendation	Taken into account / partially taken into account / not taken into account	Note
Guarantor of the EPP, Olga KOROL, candidate of technical sciences, associate professor of the cybersecurity department. Members of the EPP Working Group	Change of the specialty and field of knowledge (according to the Cabinet of Ministers of Ukraine of August 30, 2024 No 1021).	Taken into account.	Changes have been made.
Guarantor of the EPP, Olga KOROL, candidate of technical sciences, associate professor of the cybersecurity department. Members of the EPP Working Group	In order to bring it into line with modern terminology and standards of higher education, update the names of individual disciplines of the educational program.	Taken into account.	As part of the periodic review of the educational program, taking into account the recommendations of stakeholders, modern trends in the development of the industry, and updating the terminology, the names of individual academic disciplines were updated. The changes have an editorial nature and do not affect the content of disciplines, learning outcomes, the amount of ECTS credits and the structure of the educational program.
VOLOSHCHUK Olena, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.	Positive response. Without remarks.	-	-
KOVTUN Vladyslav, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.	Positive response. Without remarks.	-	-

GOLOVASHYCH Serhii, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.	Positive response. Without remarks.	-	-
OPIRSKY Ivan, Doctor of Technical Sciences, Professor, Head of the Department of Information Protection of the Institute of Computer Technology, Automation and Metrology of the National University "Lviv Polytechnic"	Positive response. Without remarks.	-	-

Head of the Department of Cybersecurity _____ Serhii YEVSEIEV

Guarantor of the educational program _____ Olga KOROL

9. PLAN TO TAKE INTO ACCOUNT THE COMMENTS AND FIX THE DEFICIENCIES UNDER THE EDUCATIONAL PROGRAM

Recommendations provided during the latest accreditation	The period (short - term/long - term/not appropriate to consider)	Measures aimed at taking into account the recommendations / justification as to Impracts of the recommendation	Terms of implementation of measures / responsible persons
General recommendations of the Expert Group and Sectoral Expert Council (in the department, industry, institute, university)			
Recommendation 1 To strengthen the information of applicants with regulatory documents and basic provisions of academic integrity.	Long -term	1) carrying out permanent explanatory work among teachers and education applicants to maintain a culture of academic integrity; 2) informing the applicants about measures to cover the issues of academic integrity, which on a permanent basis are carried out by staff of the department of quality assurance of educational activity and scientific and technical library of NTU "KPI"; 3) Periodic acquaintance of interested persons with regulatory documents, which defines the policy and procedures of compliance with academic integrity at NTU "KPI": - “Rules of conduct of education applicants at NTU“ KPI ”;	The period of time to the next accreditation of OP. Responsible: Guarantor OP, Teachers of the Department.

		- "Rules of internal regulations of NTU" KPI "; - "Code of Ethics of Academic Relations and Integrity of NTU" KPI ". 4) placement of motivational materials on the site of the Department of SIT. 5) Informing the applicants is performed constantly during the lecture classes in the discipline "Fundamentals of Scientific Research". Considered at the meeting of the department, minutes No. 12 of 14.03.2025.	
Recommendation 2 View in the next version of the APP list of approved professional standards in the field of cybersecurity in accordance with the National Classifier of Professions of Ukraine DK 003: 2010.	Long -term	Update in the OPP of the list of approved professional standards in the field of cybersecurity in accordance with the National Classifier of Professions of Ukraine DK 003: 2010. Considered at the meeting of the department, minutes No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: Guarantor OP.
Recommendation 3 Consider the possibility of introducing a dual form of education on a given EPP.	Long -term	Consider the possibility of introducing a dual form of education on a given EPP. Considered at the meeting of the department, minutes No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: Guarantor OP, Head of the Department, Teachers of the department.

Recommendation 4 Put information on VC in OPP in a convenient form for stakeholders with a clear indication of components available for choice (links to VC, table, etc.).	Long -term	To refine the information structure of the website. Developed, published and published on the department's website list of selective educational components with reference to Sylabus. Considered at the meeting of the department, minutes No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: Guarantor OP.
Recommendation 5 Involvement of students in discussion and upgrade EPP	Long -term	To meet members of the working group with representatives of student self -government. Considered at the meeting of the department, minutes No. 1 of 26.03.2025.	The period of time to the next accreditation of OP. Responsible: Guarantor OP, Head of the Department, Teachers of the department.

Director of the Educational and Scientific Institute
of Computer Science and Information Technology _____ Mykhailo HODLEVSKYI

Guarantor of the educational program _____ Olga KOROL