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"

First (bachelor) level of higher education

in specialty **F5 – Cybersecurity and information protection**
fields of knowledge **F - Information technologies**
qualification **bachelor 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	First (bachelor) level
Branch of knowledge	F Information technologies
Specialty	F5 Cybersecurity and information protection
Qualification	bachelor of cybersecurity and information protection

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

_____Sergii YEVSEIEV

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 КН-1122б

_____ Diana SIPCO

«____»_____2026

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

This educational and professional program cannot be fully or partially reproduced, reproduced and distributed without the permission of the National Technical University «Kharkiv Polytechnic Institute».

REVIEWERS:

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

1. Ivan OPIRSKY, 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. Vladyslav KOVTUN, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.
3. Serhii GOLOVASHYCH, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.
4. Olena VOLOSHCHUK, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.
5. Olga SHAPOVAL, Executive Director of Kharkiv Cluster of Information Technology

Reviews

PREFACE

Corresponds to the Standard of Higher Education of the first (bachelor) level in specialty F5 "Cybersecurity and information protection", which was approved by the order of the Ministry of Education and Science of Ukraine dated 29.10.2024 No. 1547.

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
Sergii YEVSEIEV, doctor of technical sciences, professor, head of the cybersecurity department.

Members of the workgroup EPP:
1. Olga KOROL, candidate of technical sciences, associate professor, associate professor of the cybersecurity department.
2. Serhii POHASII, doctor of technical sciences, associate professor, professor of the cybersecurity department.
3. Stanislav MILEVSKYI, doctor of technical sciences, associate professor, professor of the cybersecurity department
4. Diana SIPCO, student, group КН-1122б.

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	Bachelor Educational qualification: bachelor of cybersecurity and information protection. Diploma qualification: bachelor 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	Bachelor diploma, unitary, 240 ECTS credits, study period 3 years 10 months
Availability of accreditation	National Higher Education Quality Agency. Accreditation certificate educational program No. 9111. Valid up – 01.07.2029.
Cycle/level	first (bachelor) level of higher education; NRK of Ukraine – level 6, FQ-EHEA – first cycle, EQF LLL – level 6
Prerequisites	Persons who have received a complete general secondary education may enter to obtain a bachelor's degree in the Bachelor's Degree in F5 Cybersecurity and information protection. The reception on the basis of the degree of junior bachelor, professional junior bachelor or educational qualification level of the junior specialist is carried out in the manner prescribed by law.
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-bakalavr/

2 - The purpose of the educational and professional program	
Training of specialists capable of using and implementing information and/or cyber security technologies, as well as digital economy technologies.	
3 – Characteristics of the educational and professional program	
Subject area (field of knowledge, specialty, specialization or subject specialty (if any)	**Field of knowledge:** F "Information technologies" **Specialty:** F5 "Cybersecurity and information protection" **Object of study:** – cyber security and information protection technologies; – cyber security and information protection management processes; - security of information resources, systems and technologies, artificial intelligence, objects of information activity and critical infrastructure. **Training goals:** training specialists capable of using and implementing cyber security and information protection technologies and solving complex problems in the field of cyber security and information protection. **Theoretical content of the subject area:** theories, concepts, concepts, principles of protection of the vital interests of people, society, and the state during the use of cyberspace, security of information systems and technologies, ensuring timely detection, prevention and neutralization of targeted (mixed) attacks, objects of information activity and critical infrastructure in cyberspace. **Methods , techniques and technologies :** methods, techniques and technologies, research, modeling, analysis and improvement of the processes of creation, processing, transmission, reception, destruction, display, protection (cyber protection) of information resources, solving theoretical and practical problems of cyber security and information protection in cyberspace, detection, analysis of cyber incidents and countermeasures, prevention and neutralization of real and potential threats to information resources, objects of information activity and critical infrastructure, creation, support and ensuring the effective functioning of information protection systems, research and improvement of processes of processing and protection of information resources. **Tools and equipment :** applied and specialized software, network equipment, hardware, information protection tools and devices.
Orientation of the educational program	Educational and professional. Preparation of cybersecurity and information protection professionals.
The main focus of the educational program	Special education in the field of information technologies by specialty F5 "Cybersecurity and information protection". In-

and specialization or subject specialty (if any)	depth study of information technologies of information protection, information security, cyber security, and information security, development and use of software for information protection, cyber security, and information security. Keywords: cyber security , information security, information protection, information technologies.
Features of the program	The peculiarity of the program of specialty "Cybersecurity and information protection" is the focus on modern requirements for specialists in the field of information and/or cybersecurity, acquisition of higher education by higher education of competitive competencies based Cybersecity, Iot & Data Analytics, OS and It, Programming Courses. Ability to learn English.
4 – Eligibility of graduates to employment and academic rights of graduates	
Suitability for employment	Specialists in cybersecurity and information protection can work, according to the current version of the National classifier of Ukraine : Classifier professions DK 003:2010: 2139.2 Information security specialist; 2139.2 Safety specialist (information and communication technologies); 2139.2 Cyber defense infrastructure specialist; 2139.2 Cybersecurity Response Specialist; 2139.2 Cryptographic information specialist; 2139.2 Specialist in technical protection of information; 2139.2 Specialist in testing of security and information security systems; 2139.2 Information technology auditor (cybersecurity); 2139.2 Specialist in evaluation of information security measures (cybersecurity).
Academic rights of graduates	Students who have been trained under this curriculum and received a bachelor's degree have the right to receive education at the second (master's) higher education level in the Higher Education Institution of Ukraine and abroad in the field of knowledge "information technology" or related ones. Acquisition or improvement of education and professional training in the adult system.
5 – Teaching and assessment	
Teaching and learning	Student centered learning, problem-oriented learning, distance learning in the Microsoft 365 system, self-study, learning through project practice, learning through laboratory practice. The teaching process provides for the use of such educational technologies as: lectures, laboratory work, practical classes,

	small groups, seminars-discussions, Brainstorming, presentations that develop communicative and leadership skills, independent work with literary sources; Mixed forms of training using remote platforms.
Assessment	Monitoring of students' knowledge and skills is carried out in the form of current and final control. Current control - oral and written survey, assessment of work in small groups, testing, defense of group and individual research tasks. Final control - oral and written exams, assessments taking into account the accumulated points of the current control, defense of reports from laboratory classes, defense of coursework. State certification is a single state qualification exam. Evaluation is carried out according to the national scale ("excellent", "good", "satisfactory", "unsatisfactory"), 100-point scale and ECTS scale (A, B, C, D, E, FX, F).
6 – Software competencies	
Integral competence	The ability to solve complex specialized tasks and practical tasks in the field of cybersecurity and information protection.
General competencies (GC) (defined by the standard of higher education of the specialty)	GC1. Ability to apply knowledge in practical situations. GC2. Knowledge and understanding of the subject area and understanding of professional activity. GC3. Ability to communicate in the state language both orally and in writing. GC4. Ability to communicate in a foreign language. GC5. Ability to learn and master modern knowledge. GC6. The ability to realize own rights and responsibilities as a member of society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine. GC7. Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty. GC8. The ability to preserve and multiply moral, cultural, scientific values and achievements of society based on an understanding of the history and patterns of development of the domain, its place in the general system of knowledge about nature and society and in the development of society, technologies, to use various types and forms of motor activity for active recreation and leading a healthy lifestyle.
Special (professional) competences (SC)	SC1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and

(defined by the standard of higher education of the specialty)	standards in order to carry out professional activities in the field of cybersecurity and information protection. SC2. Ability to use information technologies, modern methods and models of cybersecurity and information security systems. SC3. Ability to ensure the continuity of business processes according to the established cybersecurity policy and information protection. SC4. Ability to protect information in information systems according to the established cybersecurity policy and information protection. SC5. The ability to restore the functioning of information systems after the realization of threats, cyberattacks, failures and failures of different classes and origin. SC6. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.). SC7. Ability to perform professional activities based on the implemented information and cyber security management system. SC8. Ability to apply methods and means of cryptographic protection of information at objects of information activity. SC9. Ability to apply methods and means of technical protection of information at objects of information activity. SC10. The ability to monitor information processes, to analyze, identify, evaluate possible vulnerability and threats to information space and information resources in accordance with the established information security policy.
7 - Learning outcomes	
The results of studies in the specialty (defined by the standard of higher education of the specialty)	LO1. Freely speak the state language orally and in writing when performing professional duties. LO2. Communicate in a foreign language in order to ensure the effectiveness of professional communication. LO3. Apply the principle of inadmissibility of corruption and any other manifestations of dishonesty in professional activity. LO4. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness. LO5. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.

	LO6. Adapt to new conditions and technologies of professional activity, predict the end result. LO7. Apply and adapt information and coding theories, mathematical statistics, numbers, cryptography and steganography, signal processing and transmission, etc., principles, methods and concepts of cybersecurity and information protection in training and professional activity. LO8. Apply knowledge and understanding of mathematics and physics in professional activity, formalize the objectives of the subject area of cybersecurity and protection of information, formulate their mathematical production and choose a rational method of solution. LO9. To know and apply the legislation of Ukraine and international requirements, practices and standards for the purpose of conducting professional activity in the field of cybersecurity and information protection. LO10. Be able to use modern information technologies, methods and models of cybersecurity and information security systems for professional activity. LO11. Plan preparation and ensure the continuity of processes in organizations according to the established cybersecurity policy and taking into account the requirements for information protection. LO12. Apply information security methods in information systems according to the established information security policy. LO13. To implement, adjust, accompany and maintain the functioning of software and software and software and software security and information protection systems as necessary procedures for the functioning of information systems and \ or infrastructure of the organization as a whole. LO14. To solve the problems of managing the recovery processes of information systems using reservation procedures according to the established security policy and to ensure the functioning of special software, to protect and restore information. LO15. Collect, process, store, analyze critical data to prove the implementation of cyber threats, analyze and research a cyberincident in order to promptly restore the functioning of the information system. LO16. To solve the problems of implementation and support of complex information protection systems in information systems. LO17. To ensure the functioning of the cybersecurity management system and the protection of the organization's

	information, including staff and managing the consequences of threats to information safety in crisis situations, on the basis of performing quantitative and qualitative risk assessment procedures. LO18. Analyze, apply the methods and means of cryptographic protection of information at information activities. LO19. To solve tasks on the organization and control of the state of cryptographic protection of information, in particular in accordance with the requirements of regulatory documents. LO20. Identify the threats of creation of technical channels of leakage of information on the objects of information activity; to implement the means and measures of technical protection of information from leakage by technical channels, to maintain and control the status of hardware means of information protection and complexes of technical protection of information. LO21. To implement, support, analysis of efficiency of systems for detecting unauthorized access, actions with information in the information system, vulnerability, possible threats to information space and information resources and use protection complexes to ensure the required level of information security in information systems.
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.
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.khpi.edu.ua/sylabusy-osvitnikh-komponentiv-f5-bakalavr/). 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 on academic mobility with universities of Ukraine. Agreements on cooperation regarding the implementation of programs of internal academic mobility of higher education students under the educational program "Cybersecurity" specialty F5 with Odesa National University of Technology, Chernihiv National University of Technology.
International credit mobility	On the basis of a bilateral agreement with the University named after Jan Dlugosha in Częstochowa (Poland).
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 educational components			
1.1 General training			
GT 1	*History and culture of Ukraine*	*4,0*	*Exam*
GT 2	*Foreign Language*	*4,0*	*Test, Exam*
GT 3	*Ukrainian as a foreign language*	*12,0*	*Test, Exam*
GT 4	*Physics*	*4,0*	*Exam*
GT 5	*Fundamentals of humanitarian and philosophical knowledge in professional activity*	*4,0*	*Exam*
GT 6	*Higher mathematics*	*6,0*	*Test*
GT 7	*Fundamentals of Higher Algebra*	*5,0*	*Exam*
GT 8	*Language of professional training*	*10,0*	*Test, Exam*
GT	*Physical education*	*4,0*	*Test*
1.2 Special (professional) training			
ST 1	*Introduction to the specialty. Introductory practice*	*3,0*	*Test*
ST 2	*Basics of programming*	*4,0*	*Exam*
ST 3	*Information and coding theory*	*3,0*	*Exam*
ST 4	*Legal Regulation of Information Security*	*4,0*	*Test*
ST 5	*Algorithms and data structures*	*5,0*	*Exam*
ST 6	*Physical bases of technical intelligence means*	*5,0*	*Test*
ST 7	*Information security of the state*	*3,0*	*Test*
ST 8	*Social Engineering Methods in Cybersecurity*	*4,0*	*Test*
ST 9	*Mathematical foundations of cryptology*	*4,0*	*Exam*
ST 10	*Programming technologies*	*5,0*	*Exam*
ST 11	*Computer networks*	*4,0*	*Exam*
ST 12	*Security of Modern Operating Systems*	*6,0*	*Exam*
ST 13	*Cybersecurity Software Development*	*6,0*	*Exam*
ST 14	*Basics of cryptographic protection*	*6,0*	*Test*
ST 15	*Fundamentals of Microprocessor System Security*	*4,0*	*Exam*
ST 16	*Mathematical Modeling of Security Systems*	*4,0*	*Exam*
ST 17	*Basics of steganographic information protection*	*5,0*	*Exam*
ST 18	*DevOps Security*	*4,0*	*Test*
ST 19	*Web application development*	*6,0*	*Exam*

ST 20	*Integrated information security systems*	*5,0*	*Exam*
ST 21	*Web security*	*5,0*	*Exam*
ST 22	*Comprehensive training*	*4,0*	*Test*
ST 23	*Neural Networks*	*4,0*	*Test*
ST 24	*Open Source Intelligence (OSINT)*	*3,0*	*Test*
2. Practical training			
PT 1	*Industrial practice*	*6,0*	*Test*
PT 2	*Technological practice*	*6,0*	*Test*
3. Attestation			
	Attestation	*3,0*	
General amount mandatory components		***174***	
4. Optional educational components			
4.1 Specialised training			
Profiled package of educational components 01 "Artificial Intelligence in Security Systems"			
EC 1.1	*Ethical hacking*	*3,0*	*Exam*
EC 1.2	*Date of mining*	*3,0*	*Exam*
EC 1.3	*Mathematical foundations of artificial intelligence*	*3,0*	*Exam*
EC 1.4	*Python for artificial intelligence and machine learning*	*4,0*	*Exam*
EC 1.5	*Genetic algorithms*	*4,0*	*Exam*
EC 1.6	*Python for internet things*	*3,0*	*Exam*
EC 1.7	*Systems engineering*	*3,0*	*Exam*
Profiled package of educational components 02 "Blockchain technology and security of banking systems"			
EC 2.1	*Decentralised systems*	*3,0*	*Exam*
EC 2.2	*Risk management*	*3,0*	*Exam*
EC 2.3	*Blockchain: basics and application examples*	*3,0*	*Exam*
EC 2.4	*Security of banking systems*	*4,0*	*Exam*
EC 2.5	*Protecting critical infrastructure facilities*	*4,0*	*Exam*
EC 2.6	*Organising document management with restricted access*	*3,0*	*Exam*
EC 2.7	*Security in social networks*	*3,0*	*Exam*
Profiled package of educational components в 03 "Innovation Campus"			
EC 3.1	*Basics of cybersecurity*	*3,0*	*Exam*
EC 3.2	*Development of corporate information systems (part 1)*	*3,0*	*Exam*
EC 3.3	*Development of corporate information systems (part 2)*	*3,0*	*Exam*
EC 3.4	*Databases for corporate information systems*	*4,0*	*Exam*
EC 3.5	*Architecture of corporate information systems*	*4,0*	*Exam*
EC 3.6	*Security and audit of wireless and mobile networks*	*3,0*	*Exam*

EC 3.7	*Protecting critical infrastructure facilities*	*3,0*	*Exam*
4.2 Educational components of free choice of professional training of the general institute catalog			
ECPT 1	*EC FC PT 1*	*4,0*	*Test*
ECPT 2	*EC FC PT 2*	*4,0*	*Test*
ECPT 3	*EC FC PT 3*	*4,0*	*Test*
ECPT 4	*EC FC PT 4*	*4,0*	*Test*
ECPT 5	*EC FC PT 5*	*4,0*	*Test*
ECPT 6	*EC FC PT 6*	*4,0*	*Test*
ECPT 7	*EC FC PT 7*	*4,0*	*Test*
4.3 Educational components of free choice of general training			
ECGT 1	*EC FC GT 1*	*4,0*	*Test*
ECGT 2	*EC FC GT 2*	*4,0*	*Test*
ECGT 3	*EC FC GT 3*	*4,0*	*Test*
4.4 Educational components of special university choice			
ECSUC	*ECSUC*	*3,0*	*Test*
Total amount for elective components:		***66***	
GENERAL SCOPE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM:		***240***	

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	53 / 22,1	-	**53 / 22,1**
2	Special (professional) training	106/ 44,2	-	**106/ 44,2**
3	Practical training	12/5	-	**12/5**
4	Attestation	3/1,2	-	**3/1,2**
5	Optional educational components	-	66 / 27,5	**66 / 27,5**
Total for the entire term teaching		**174 / 72,5**	**66 / 27,5**	**240 / 100**

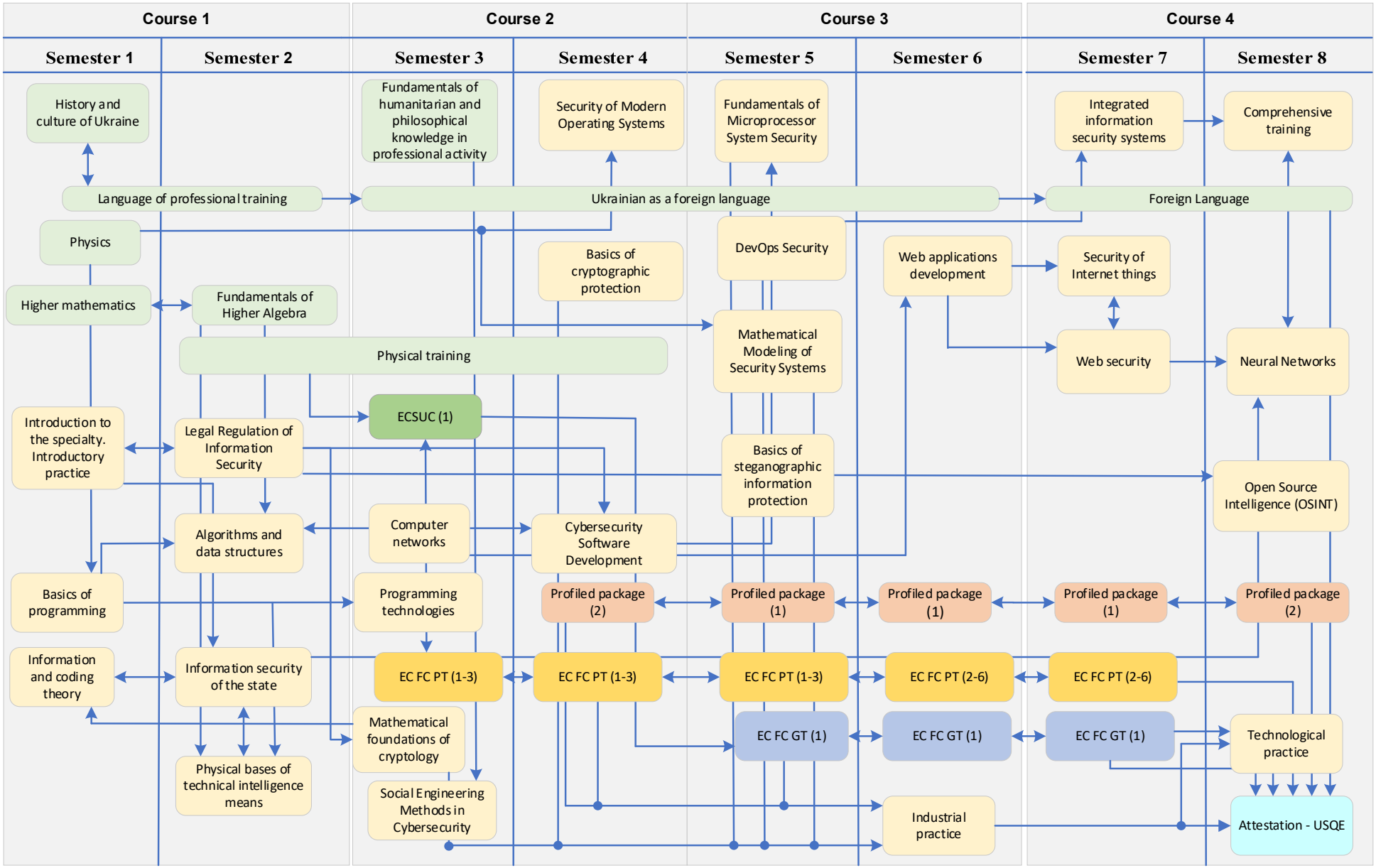
4. FORM CERTIFICATES EARNERS HIGHER EDUCATION

Forms of attestation of applicants of higher education	Attestation is carried out in the form of a state qualification exam.
Requirements for the unified state qualification exam	The only state qualification exam provides for evaluating the achievements of the learning outcomes, defined by the higher education standard of the specialty "Cybersecurity and information protection" and the educational program.

PROJECT

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

5. STRUCTURAL AND LOGICAL SCHEME



PROJECT

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

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** **Зн1.** Conceptual scientific and practical knowledge. **Зн2.** Critical understanding of theories, principles, methods and concepts in the field of professional activity and/or learning.	**Skill** **Ум1.** Deep cognitive and practical skills, skills and innovation at the level necessary to solve complex specialized tasks and practical problems in the field of professional activity or learning.	**Communication** **К1.** Reporting to experts and non -specialists of information, ideas, problems, solutions to their own experience and argumentation. **К2.** Collection, interpretation and use of data. **К3.** Communication on professional issues, including foreign language.	**Responsibility and autonomy** **АВ1.** Management of complex technical or professional activities or projects. **АВ2.** The ability to be responsible for making and making decisions in unpredictable working and/or educational contexts. **АВ3.** Formation of judgments that take into account social, scientific and ethical aspects. **АВ4.** Organization and management of professional development of persons and groups. **АВ5.** The ability to continue learning with a significant degree of autonomy.
GENERAL COMPETENCES				
GC 1	Зн2	Ум1		
GC 2	Зн2	Ум1	К1	
GC 3			К1, К3	
GC 4			К1, К3	
GC 5	Зн1, Зн2	Ум1	К2	АВ3
GC 6	Зн1		К1	АВ2, АВ3, АВ4
GC 7			К1	АВ2
GC 8	Зн2		К2	АВ3
SPECIAL (PROFESSIONAL) COMPETENCES				
SK1	Зн2	Ум1	К2	
SK2	Зн1, Зн2	Ум1	К2	
SK3		Ум1		АВ1
SK4		Ум1		АВ1
SK5		Ум1	К2	АВ1, АВ2
SK6		Ум1	К1	АВ1
SK7		Ум1	К1	АВ1
SK8	Зн2	Ум1		
SK9	Зн2	Ум1		

SK10		Ум1	К2	АВ2

6. MATRIX OF MATCHING DEFINED OF STANDARD LEARNING OUTCOMES, COMPETENCIES AND EDUCATIONAL COMPONENTS

Learning outcomes	Competences																	
	Integral competenc	General competences								Special (professional) competences								
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
LO1	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22			GT6 GT7 ST1 ST2 ST5 ST6 ST7 ST8 ST10 ST11 ST13 ST14 ST17 ST18 ST20 ST24 PT1 PT2															

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO2	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22				GT2 GT3 ST7 ST8 ST11 ST12 ST14 ST24														

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO3	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22						GT1 ST1 ST4 ST7	ST4 ST7											

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO4	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22	GT4 GT ST2 ST3 ST4 ST5 ST7 ST8 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST19 ST21 ST22 ST23 ST24 PT1 PT2	GT4 GT5 GT6 GT7 ST1 ST2 ST4 ST5 ST6 ST7 ST10 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 PT1 PT2																	

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO5	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22	GT4 GT ST2 ST3 ST4 ST5 ST7 ST8 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST19 ST21 ST22 ST23 ST24 PT1 PT2	GT4 GT5 GT6 GT7 ST1 ST2 ST4 ST5 ST6 ST7 ST10 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 PT1 PT2																	

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO6	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22		GT4 GT5 GT6 GT7 ST1 ST2 ST4 ST5 ST6 ST7 ST10 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 PT1 PT2						GT1 GT4 GT5 GT ST1 ST3 ST17 ST20 ST23										

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO7	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22	GT4 GT ST2 ST3 ST4 ST5 ST7 ST8 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST19 ST21 ST22 ST23 ST24 PT1 PT2							GT1 GT4 GT5 GT ST1 ST3 ST17 ST20 ST23										

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO8	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22					GT4 GT6 GT7 ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST23														

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO9	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22						GT1 ST1 ST4 ST7			ST1 ST4 ST7 ST8 ST10 ST11 ST14 ST20 ST23 ST24									

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO10	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22										ST2 ST3 ST5 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 PT1									

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO11	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22											ST11 ST14 ST20 ST21 ST24								

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO12	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22												ST9 ST11 ST12 ST14 ST19 ST20 ST21 ST22 ST23 ST24								

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO13	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22												ST9 ST11 ST12 ST14 ST19 ST20 ST21 ST22 ST23 ST24								

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO14	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22													ST8 ST11 ST14 ST15 ST21 ST24					

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO15	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22													ST8 ST11 ST14 ST15 ST21 ST24					

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO16	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22														ST11 ST12 ST14 ST20 ST23 PT2				

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO17	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22															ST7 ST16 ST23 PT1 PT2			

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO18	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22																ST3 ST9 ST11 ST12 ST14 ST15 ST18 ST21 ST23 ST24 ПП2		

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO19	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22																ST3 ST9 ST11 ST12 ST14 ST15 ST18 ST21 ST23 ST24 ПП2		

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO20	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22																	ST6 ST12 ST14 ST15 ST19 ST20 ST22 ST23 PT2	

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		
LO21	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22																		ST8 ST11 ST14 ST16 ST18 ST23 ST24 PT1

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 PT1 PT2																		

7. THE RESULTS OF DISCUSSING THE EDUCATIONAL PROGRAM

Stakeholders	Remarks / Recommendation	Taken into account / partially taken into account / not taken into account	Note
Olga SHAPOVAL, Executive Director of Kharkiv Cluster of Information Technology	Pay more attention to mastering security principles in databases. Emphasis on the study of cloud technologies and Devops.	Taken into account.	Due to the selective educational components: Security in Devops, databases with SQL and Python
Guarantor of the EPP, Sergii YEVSEIEV, doctor of technical sciences, professor, head of the cybersecurity department. Members of the EPP Working Group	Educational and professional program to comply with the requirements of the Higher Education Standard in the specialty 125 Cybersecurity and information protection of the first (bachelor) level of higher education, approved and put into force by the order of the Ministry of Education and Science of Ukraine dated 24.10.2024. No. 1547.	Taken into account.	Educational and professional program to comply with the requirements of the Higher Education Standard in the specialty 125 Cybersecurity and information protection of the first (bachelor) level of higher education, approved and put into force by the order of the Ministry of Education and Science of Ukraine dated 24.10.2024. No. 1547.
Guarantor of the EPP, Sergii YEVSEIEV, doctor of technical sciences, professor, head 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.
Olena VOLOSHCHUK, Candidate of Technical	Positive response. Without remarks.	-	-

Sciences, Head of Educational Programs of Distributed Lab LLC.			
Ivan OPIRSKY, 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.	-	-
Vladyslav KOVTUN, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.	Positive response. Without remarks.	-	-
Serhii GOLOVASHYCH, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.	Positive response. Without remarks.	-	-

Head of the Department of Cybersecurity _____ Serhii YEVSEIEV

Guarantor of the educational program _____ Serhii YEVSEIEV

8. PLAN TO TAKE INTO ACCOUNT THE COMMENTS/RECOMMENDATIONS ON THE RESULTS OF THE ACCREDITATION EXAMINATION OF 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)			
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 EPP 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, Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: guarantor OP.
To strengthen students' awareness of internal procedures for organizing the educational process. It is recommended to review and update literature in the syllabus of educational components.	Long -term	To strengthen students' awareness of internal procedures for organizing the educational process. It is recommended to review and update literature in the syllabus of educational components. Considered at the meeting of the department, Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: Head of the Department, teachers of the department.
Using a cyberpoligon to familiarize students with his capabilities	Long -term	Using a cyberpoligon to familiarize students with his capabilities.	The period of time to the next accreditation of OP.

		Considered at the meeting of the department, Protocol No. 12 of 14.03.2025.	Responsible: guarantor OP, Head of the Department.
Provide constant updating of information on all aspects of EPP proceedings on the department's website.	Long -term	Updating information on all aspects of EPP proceedings on the department's website. Considered at the meeting of the department, Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: guarantor OP.

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

Guarantor of the educational program _____ Serhii YEVSEIEV