MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
STATE UNIVERSITY OF INFORMATION
AND COMMUNICATION TECHNOLOGIES

Project

EDUCATIONAL PROGRAM

“CYBERSECURITY AND INFORMATION PROTECTION MANAGEMENT”

of the first (bachelor’s) level of higher education

Specialty	**F5 Cybersecurity and Information Protection**
Field of Knowledge	**F Information Technologies**
Qualification:	**Bachelor in Cybersecurity and Information Protection**

APPROVED BY THE ACADEMIC COUNCIL OF THE UNIVERSITY
Minutes №
Order №

Rector_____ Volodymyr SHULHA

Kyiv – 2026

LETTER OF APPROVAL

OF THE EDUCATIONAL PROGRAM
FOR THE TRAINING OF HIGHER EDUCATION APPLICANTS

Field of Knowledge	F "Information Technologies"
Specialty	F5 "Cybersecurity and Information Protection"
Level of Higher Education	First (Bachelor's)
Qualification	Bachelor in Cybersecurity and Information Protection

1. First Vice-Rector Oleksandr KORCHENKO

2. Vice-Rector for Educational Work Artur GUDMANIAN

3. Acting Head of the Educational and Methodical Department. Vadym VLASENKO

4. Academic Council of the Educational-Scientific Institute of Cyber security and Information Protection

Minutes	№		date				

Chair of the Academic Council of the ESICIP _____Yevheniia IVANCHENKO

5. Department of Cybersecurity and Information Protection Management

Minutes	№		date				

Head of the Department
of Cybersecurity and Information
Protection Management _____ Svitlana LEHOMINOVA

Head of the Student Council of the ESICIP _____ Stanislav SHTEFAN

Reviews from external stakeholders (partner companies):

PREFACE

Developed by the working group consisting of:

Guarantor of the Educational Program –
Dmytro RABCHUN - Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity and Information Protection Management.

Members of the working group:
Svitlana LEHOMINOVA - Doctor of Economic Sciences, Professor, Head of the Department of Cybersecurity and Information Protection Management;
Vitalii SAVCHENKO - Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Information Protection Management;
Tetiana MUZHANOVA - Candidate of Sciences in Public Administration, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection Management;

Diana PRYMACHENKO – applicant for higher education of the third (educational and scientific) level in Specialty F5 “Cybersecurity and Information Protection”;
Oleksandr SKRYPKA – applicant for higher education of the second level in Specialty F5 “Cybersecurity and Information Protection”;
Oleksii MOROZOV – Director of LLC “IT Specialist”;
Yurii LYSETSKYI – Director of SE “S&T Ukraine”.

.

INFORMATION ON THE REVIEW OF THE EDUCATIONAL PROGRAM

Developed for the first time in accordance with:

The State Standard of Higher Education for Specialty 125 “Cybersecurity” of the Field of Knowledge 12 “Information Technologies” for the first (bachelor’s) level of higher education (Order of the Ministry of Education and Science of Ukraine dated 04.10.2018 № 1074);

Order of the Ministry of Education and Science of Ukraine № 1547 dated October 29, 2024 “On Amendments to the Standard of Higher Education in Specialty “Cybersecurity” of the Field of Knowledge 12 “Information Technologies” for the first (bachelor’s) level of higher education.”

Profile of the Educational Program

1 – General Information	
Full name of the higher education institution and structural unit	State University of Information and Communication Technologies, Educational-Scientific Institute of Cyber security and Information Protection
Degree of higher education and title of qualification in the original language	Bachelor Educational qualification – Bachelor in Cybersecurity and Information Protection
Official title of the educational program	Educational Program – Cybersecurity and Information Protection Management
Type of diploma and volume of the educational program	Bachelor's diploma, single: based on complete general secondary education – volume of the educational program: 240 ECTS credits (duration of study: 3 years and 10 months full-time; 4 years and 10 months part-time); based on the obtained educational degrees of junior bachelor, professional junior bachelor (educational-qualification level of junior specialist), the higher education institution has the right to recognize and re-credit no more than 60 ECTS credits obtained within the previous educational program of specialist training.
Accreditation availability	Introduced from September 1, 2025 for the first time (not accredited)
Cycle/level	NQF of Ukraine – Level 6 / Bachelor, QF-EHEA – first cycle, EQF-LLL – Level 6
Prerequisites	Availability of a certificate of complete general secondary education or a diploma of junior bachelor, professional junior bachelor (educational-qualification level of junior specialist).
Language(s) of instruction	Ukrainian, English
Validity period of the educational program	The program is planned to be introduced on September 1, 2025 and may be adjusted in accordance with the "Regulation on the Introduction and Updating of Educational Programs at the State University of Information and Communication Technologies".
Internet address of the permanent placement of the educational program description	https://duikt.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

2 – Purpose of the Educational Program	
The purpose of the bachelor's program is the formation and development of general and professional competencies in specialists capable of using and implementing cybersecurity and information protection technologies and solving complex tasks in the field of cybersecurity and information protection, specifically focusing on cybersecurity management with the right to further professional activity in state and private enterprises and organizations, which will contribute to the sustainable social development of the information society and the neutralization of real and potential threats to the national security of Ukraine in cyberspace.	
3 – Characteristics of the Educational Program	
Subject area, direction (field of knowledge, specialty)	F Information Technologies F5 Cybersecurity and Information Protection
Orientation of the educational program	Educational. 100% of the volume of the educational program is aimed at ensuring general and special (professional, subject) competencies in Specialty F5 Cybersecurity and Information Protection, as defined by the higher education standard. The program is applied in nature, aimed at meeting the needs of the labor market, particularly in the IT field.
Main focus of the educational program and specialization	Special education and professional training in the field of information technologies. – Training of specialists capable of using and implementing cybersecurity and information protection technologies at enterprises and organizations; cybersecurity and information protectionmanagement processes at objects of information activity and critical infrastructure objects, including information and information-communication systems, information resources and technologies. Keywords: CYBERSECURITY, MANAGEMENT, INFORMATION, RISKS, THREATS, VULNERABILITIES, INCIDENTS, PROTECTION.
Description of the subject area	The program provides for the teaching of educational components by specialists in cybersecurity and its information-analytical support, which significantly strengthens the special, professional, and subject competencies of future specialists. Lecture courses, seminars, practical and laboratory classes are conducted with the involvement of cybersecurity practitioners. **Objects of study:** – cybersecurity and information protection technologies; – cybersecurity and information protection management

	processes; information activity objects, including information and information-communication systems, information resources and technologies **Learning objectives:** Training specialists capable of using and implementing cybersecurity and information protection technologies. **Theoretical content of the subject area:** Principles, concepts, theories of protecting vital interests of individuals, society, and the state during the use of cyberspace, ensuring sustainable development of the information society and the digital communication environment, and timely detection, prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace. **Methods, methodologies, and technologies:** Methods, methodologies, and technologies for solving theoretical and practical tasks of cybersecurity and information protection. **Tools and equipment:** Means, devices, network equipment, application and specialized software, information systems and complexes for designing, modeling, control, monitoring, storage, processing, visualization, and protection of data (information flows).
Employment of graduates	To positions in structural units of institutions / enterprises / organizations that require higher education in Specialty F5 Cybersecurity and Information Protection.
Specific features of the program	The program provides for: – teaching of components of the professional training cycle in English; – obtaining certificates from leading companies in the field of information technologies within the educational process; – involvement of practitioners in information and cybersecurity in conducting seminars, practical and laboratory classes; – ensuring conditions for the training of higher education applicants in the real environment of their future professional activity to acquire relevant competencies through the organization of practices (introductory, industrial, and pre-diploma) in partner organizations and companies with the possibility of further employment.
4 – Suitability of graduates for employment and further study	
Suitability for employment	A Bachelor in Cybersecurity and Information Protection under the educational program “Cybersecurity and

	Information Protection Management" is able to perform professional work according to the National Classifier of Occupations DK 003:2010: **Primary:** 2139.2 – Information Protection Specialist; 2139.2 – Security Specialist (information and communication technologies); 2139.2 – Information Technology Auditor (in cybersecurity). **Additional** : 2139.2 – Specialist in the assessment of information protection (cybersecurity) measures .
Academic rights of graduates	Have the right to obtain education at the second (master's) level of higher education. Acquisition or improvement of education and professional training within the adult education system.
5 – Teaching and assessment	
Teaching and learning	Student-centered learning and teaching. Teaching is conducted in the state language. Certain disciplines that form professional competencies are taught in a foreign language (English). Teaching is aimed at the acquisition of knowledge, abilities and skills for further application in practice. The main ways of delivering the content of the educational program are lectures, practical classes, laboratory classes, seminars and individual lessons, consultations, solving situational tasks, testing, presentations, introductory, industrial, and pre-graduation internships.
Assessment	Types of control: ongoing, intermediate (modular, thematic), and final control. Assessment of acquired competencies is carried out during control activities provided for by this educational program and specified in the curriculum. The criteria for assessing the knowledge, abilities, and skills of higher education applicants are developed in accordance with current legislation and approved in the "Regulation on the Organization of the Educational Process at the State University of Information and Communication Technologies." Additionally, for the purpose of earning extra points within disciplines, certificates obtained by students from well-known companies in the subject area of the disciplines are taken into account.

6 - Program Competencies	
Integrated competency	The ability to solve complex specialized and practical tasks in the field of cybersecurity and information protection.
General competencies (GC)	**GC1.** The ability to apply knowledge in practical situations. **GC2.** Knowledge and understanding of the subject area and understanding of professional activity. **GC3.** The ability to communicate in the state language both orally and in writing. **GC4.** The ability to communicate in a foreign language. **GC5.** The ability to learn and master modern knowledge. **GC6.** The ability to exercise one's rights and responsibilities as a member of society, to understand the values of a civic (free democratic) society and the necessity of its sustainable development, the rule of law, and the rights and freedoms of individuals and citizens in Ukraine. **GC7.** The ability to make decisions and act following the principle of zero tolerance for corruption and any other manifestations of dishonesty. **GC8.** The ability to preserve and multiply moral, cultural, and scientific values and achievements of society based on understanding the history and regularities of the development of the subject area, its place in the general system of knowledge about nature and society, and in the development of society, technology, and engineering; the ability to use various types and forms of physical activity for active recreation and a healthy lifestyle.
Special (professional, subject) competencies (SC)	**SC1.** The ability to apply legislative and regulatory frameworks, as well as national and international requirements, practices, and standards in professional activities. **SC2.** The ability to use information technologies, modern methods and models of cybersecurity, and information protection systems. **SC3.** The ability to ensure business continuity in accordance with the established cybersecurity and information protection policy. **SC4.** The ability to ensure information protection in information and information-communication systems in accordance with the established cybersecurity and information protection policy. **SC5.** The ability to restore the functioning of information and information-communication systems after threats, cyberattacks, failures, and malfunctions of various classes

	and origins. **SC6.** The ability to implement and ensure the operation of integrated information protection systems (complexes of regulatory, organizational, and technical measures and methods, procedures, practical techniques, etc.). **SC7.** The ability to perform professional activities based on an implemented information and cybersecurity management system. **SC8.** The ability to apply methods and tools of cryptographic information protection on objects of information activity. **SC9.** The ability to apply methods and tools of technical information protection on objects of information activity. **SC10.** The ability to monitor information processes, analyze, identify, and assess possible vulnerabilities and threats to the information space and information assets in accordance with the established information security policy.
7 – Program Learning Outcomes (PLOs)	
	PLO1. Communicate freely in the state language orally and in writing when performing professional duties. **PLO2.** Communicate in a foreign language to ensure effective professional communication. **PLO3.** Apply the principle of zero tolerance for corruption and any other manifestations of dishonesty in professional activity. **PLO4.** Organize one's professional activity, select and use optimal methods and approaches to solve complex specialized tasks and practical problems in professional activity, and evaluate their effectiveness. **PLO5.** Analyze, reason, and make decisions when solving complex specialized and practical tasks in professional activity characterized by complexity and incomplete determination of conditions, and take responsibility for the decisions made. **PLO6.** Adapt to new conditions and technologies of professional activity, and predict the final outcome. **PLO7.** Apply and adapt theories of information and coding, mathematical statistics, numbers, cryptography and steganography, signal processing and transmission, as well as principles, methods, and concepts of cybersecurity and information protection in learning and professional activity. **PLO8.** Apply knowledge and understanding of mathematics and physics in professional activity,

	formalize tasks in the subject area of cybersecurity and information protection, formulate their mathematical representation, and choose a rational method for solving them. **PLO9.** Know and apply the legislation of Ukraine and international requirements, practices, and standards to carry out professional activity in the field of cybersecurity and information protection. **PLO10.** Use modern information technologies, methods, and models of cybersecurity and information protection systems for professional activity. **PLO11.** Plan preparation and ensure business continuity in organizations in accordance with established cybersecurity policy, considering information protection requirements. **PLO12.** Apply methods and tools for information protection in information and information-communication systems in accordance with established information security policy. **PLO13.** Implement, configure, maintain, and support the functioning of software and hardware-software complexes and cybersecurity and information protection systems as necessary procedures for the operation of information and information-communication systems and/or the organization's infrastructure as a whole. **PLO14.** Solve management tasks for restoring normal functioning of information and information-communication systems using backup procedures in accordance with established security policy and ensure the functioning of specialized software for information protection and recovery. **PLO15.** Collect, process, store, and analyze critical data for proving the implementation of cyber threats, conduct analysis and investigation of cyber incidents to promptly restore the functioning of an information system. **PLO16.** Solve tasks related to the implementation and maintenance of integrated information protection systems in information systems. **PLO17.** Ensure the functioning of the organization's cybersecurity and information protection management system, including personnel and managing the consequences of information security threats in crisis situations, based on the implementation of quantitative and qualitative risk assessment procedures. **PLO18.** Analyze and apply methods and tools of cryptographic information protection on objects of

	information activity. **PLO19.** Solve tasks related to the organization and control of the state of cryptographic information protection, including in accordance with the requirements of regulatory documents. **PLO20.** Identify threats of technical information leakage channels on objects of information activity; implement means and measures of technical information protection against leakage through technical channels; maintain and control the state of hardware information protection tools and technical protection complexes. **PLO21.** Implement, support, and analyze the effectiveness of systems for detecting unauthorized access, information actions in an information system, vulnerabilities, possible threats to the information space and information assets, and use protection complexes to ensure the required level of information security in information systems.
8 – Resource Support for Program Implementation	
Staffing	All academic staff involved in the implementation of the educational component of the educational-professional program are full-time employees of the State University of Information and Communication Technologies and have a confirmed level of scientific and professional activity. The support team for the F5 Cybersecurity and Information Protection specialty is formed from among the academic staff of the State University of Information and Communication Technologies. The quantitative and qualitative composition of the team complies with Licensing Requirements.
Material and technical support	For conducting practical and laboratory classes aimed at forming specialized competencies in the F5 Cybersecurity and Information Protection specialty of the Educational Program "Cybersecurity and Information Protection Management," specialized laboratories of the State University of Information and Communication Technologies are used, equipped with modern computers and hardware-software complexes. TRAINING LABORATORY FOR CYBER INCIDENT RESPONSE The laboratory is intended for conducting practical classes using hardware-software complexes: USM/SIEM from AlienVault vendor, IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional. The laboratory allows practicing skills in a Security Operation

	Center (SOC) using technologies for monitoring, detection, analysis, and response to cyber incidents in corporate information systems. TRAINING LABORATORY FOR NETWORK SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES CISCO The laboratory is intended for studying CISCO network security technologies, conducting trainings on implementing HoneyPot technology to counter cyberattacks on corporate information systems, and certification courses from the department's partner – CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. The laboratory was created with the assistance of CISCO. TRAINING LABORATORY SECURITY OPERATION CENTER The laboratory is intended for conducting practical classes on analysis, processing, and auditing of information security and/or cybersecurity using SIEM systems and software scanners such as Nessus and Kali Linux. In addition, the laboratory is used to study risk management methods based on CRAMM, OCTAVE, and RiskWatch methodologies in accordance with the requirements of international standards for information security and/or cybersecurity.
Information and educational-methodical support	Information about the educational program, its educational components, and the requirements for persons eligible to study in this program is posted on the official website of the State University of Information and Communication Technologies. All educational components of the program are provided with teaching and methodological materials and are freely available as library resources, the electronic library of the State University of Information and Communication Technologies, and the Google Classroom learning management system.
9 – Academic Mobility	
National credit mobility	The existence of bilateral agreements between SUICT and higher education institutions in Ukraine ensures national credit mobility.
International credit mobility	The curriculum corresponds to global educational standards, allowing students to participate in dual degree programs and be competitive in the global labor market.
Education of international students	–

2. List of Educational Program Components and Their Logical Sequence

2.1. Training Content by Educational Program, Competencies, and Learning Outcomes

№	Component	Code	Competence	Learning Outcome
1. Cycle of General Education Components				
1.	Higher Mathematics	EC01	IC, GC5	PLO8
2.	Fundamentals of Information and Cybersecurity Management	EC02	IC, GC6, SC1, SC2, SC3	PLO9, PLO10, PLO11
3.	Business Analytics in Cybersecurity	EC03	IC, GC1, GC2	PLO4
4.	Philosophy	EC04	IC, GC3	PLO1
5.	Foreign Language*	EC05	IC, GC4	PLO2
6.	Ukrainian Language for Professional Purposes	EC06	IC, GC3	PLO1
7.	Communications in Cybersecurity and Information Protection	EC07	IC, GC1, GC2, GC6, GC7	PLO3, PLO4
8.	Socio-Ecological Safety of Life	EC08	IC, GC2, GC6, GC7, GC8	PLO3, PLO6
9.	Regulatory and Legal Support of Information Security	EC09	IC, GC6, SC1	PLO 9
10.	Physics	EC10	IC, GC8	PLO8
11.	Information and Coding Theory	EC11	IC, GC1, GC8	PLO7
12.	End Devices of Information Systems	EC12	IC, GC 2, GC8	PLO2, PLO6
13.	Theoretical Training of Basic Military Training	EC13	IC, GC 6, GC 8	PLO 3, PLO 6, PLO 9
2. Cycle of Professional and Practical Training Components				
1.	Theory of Circuits and Signals in Information and Cyberspace	EC14	IC, GC1, GC2, GC5, SC9	PLO5, PLO8, PLO20
2.	Applied Programming	EC15	IC, GC1, GC2, GC5	PLO5, PLO8
3.	Information and Cybersecurity Standards	EC16	IC, GC6, SC1	PLO9
4.	Operating Systems	EC17	IC, GC 3, GC8, SC2	PLO6, PLO10

5.	Analysis and Assessment of Information Systems Vulnerabilities	EC18	IC, SC10	PLO21
6.	Protection Against Malicious Software	EC19	IC, SC2, SC4	PLO10, PLO12, PLO13
7.	Applied Cryptology	EC20	IC, GC1, GC8, SC8	PLO7, PLO18, PLO19
8.	Cloud Technologies	EC21	IC, SC2	PLO10
9.	Comprehensive Information Protection Systems	EC22	IC, SC6, SC9	PLO16, PLO20
10.	Artificial Intelligence	EC23	IC, GC1, GC2, SC2	PLO5, PLO10
11.	Fundamentals of National Security	EC24	IC, GC2, GC6, GC7, SC1	PLO3, PLO4, PLO5, PLO9
12.	State Information Security	EC25	IC, GC2, GC6, GC7, SC1	PLO3, PLO4, PLO5, PLO9
13.	Information Security Management System	EC26	IC, SC3, SC 7	PLO 2, PLO11, PLO17
14.	Risk Theory	EC27	IC, SC7	PLO17
15.	Systems Analysis of Information Security	EC28	IC, SC7	PLO17
16.	Digital Forensics	EC29	IC, SC2, SC5	PLO10, PLO14, PLO15
17.	Economic Security of Enterprise Activities	EC30	IC, SC3	PLO11
18.	SIEM Systems	EC31	IC, SC2, SC5	PLO10, PLO12, PLO13
19.	Organizational Support for Information Protection	EC32	IC, SC3, SC4	PLO11, PLO12, PLO13
20.	Organization of Confidential Record Keeping	EC33	IC, GC1, GC4, GC6, GC7	PLO1, PLO2, PLO3
21.	Information Security Management Systems Audit	EC34	IC, SC10	PLO21
22.	Strategic Communications	EC35	IC, GC1, GC2, GC4, SC1	PLO2, PLO4, PLO9
23.	Information Security Policies	EC36	IC, SC1, SC3, SC7	PLO9, PLO11, PLO17

24.	Introductory Practice	EC37	IC, GC1, GC2, GC6, GC8, SC1, SC2	PLO4, PLO6, PLO9, PLO10
25.	Industrial Practice	EC38	IC, GC1, GC2, GC5,GC6, GC7, GC8, SC1, SC2, SC3	PLO3, PLO4, PLO6, PLO7, PLO8, PLO9, PLO10, PLO11
26.	Pre-Diploma Practice	EC39	IC, GC1, GC2, GC5,GC6, GC7, GC8, SC1, SC2, SC3,SC4,SC5	PLO3, PLO4, PLO6, PLO7, PLO8, PLO9, PLO10, PLO11, PLO12, PLO13, PLO14, PLO15
27.	Qualification Work	EC40	IC, GC1, GC2, GC5,GC6, GC7, GC8, SC1, SC2, SC3,SC4, SC5, SC7, SC10	PLO3, PLO4, PLO6, PLO7, PLO8, PLO9, PLO10, PLO11, PLO12, PLO 13, PLO14, PLO15, PLO17, PLO21
3. Student-Selected Elective Courses				
1.	Student-Selected Component			
2.	Student-Selected Component			
3.	Student-Selected Component			
4.	Student-Selected Component			
5.	Student-Selected Component			
6.	Student-Selected Component			
7.	Student-Selected Component			
8.	Student-Selected Component			
9.	Student-Selected Component			
10.	Student-Selected Component			
11.	Student-Selected Component			
12.	Student-Selected Component			

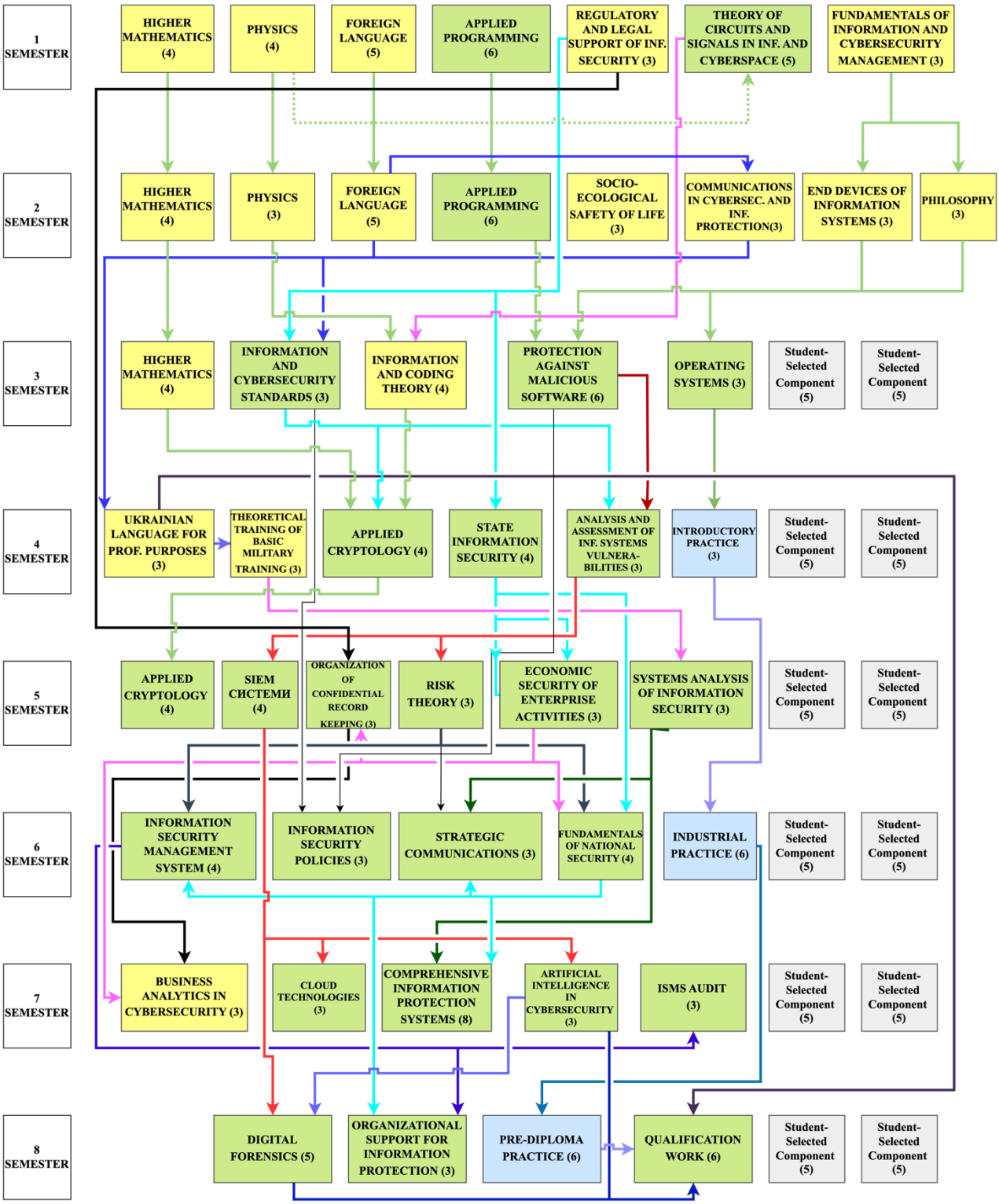
* Foreign language courses in curricula for international students and stateless persons are replaced with Ukrainian (for professional purposes).

2.2. List of Educational Program Components

Code	Component of the Educational Program (courses, projects, practical training, qualification work)	Credits	Form of Final Assessment
1	2	3	4
Mandatory Components of the Educational Program			
EC1	Higher Mathematics	12	Credit, Credit, Exam
EC2	Fundamentals of Information and Cybersecurity Management	3	Credit
EC3	Business Analytics in Cybersecurity	3	Credit
EC4	Philosophy	3	Exam
EC5	Foreign Language*	10	Credit, Exam
EC6	Ukrainian Language for Professional Purposes	3	Credit
EC7	Communications in Cybersecurity and Information Protection	3	Credit
EC8	Socio-Ecological Safety of Life	3	Exam
EC9	Regulatory and Legal Support of Information Security	3	Exam
EC10	Physics	7	Credit, Exam
EC11	Information and Coding Theory	4	Exam
EC12	End Devices of Information Systems	3	Credit
EC13	Theoretical Training of Basic Military Training	3	Credit
EC14	Theory of Circuits and Signals in Information and Cyberspace	5	Exam
EC15	Applied Programming	10	Credit, Exam
EC16	Information and Cybersecurity Standards	3	Exam
EC17	Operating Systems	3	Exam
EC18	Analysis and Assessment of Information Systems Vulnerabilities	3	Exam, Term paper
EC19	Protection Against Malicious Software	6	Credit
EC20	Applied Cryptology	8	Credit, Exam Term paper
EC21	Cloud Technologies	3	Credit
EC22	Comprehensive Information Protection Systems	8	Exam, Term paper
EC23	Artificial Intelligence in Cybersecurity	3	Exam
EC24	Fundamentals of National Security	4	Exam
EC25	State Information Security	4	Exam
EC26	Information Security Management System	4	Exam, Term paper
EC27	Risk Theory	3	Credit
EC28	Systems Analysis of Information Security	3	Credit
EC29	Digital Forensics	5	Exam
EC30	Economic Security of Enterprise Activities	3	Credit
EC31	SIEM Systems	4	Exam
EC32	Organizational Support for Information Protection	3	Exam

EC33	Organization of Confidential Record Keeping	3	Credit
EC34	Information Security Management Systems Audit	3	Credit
EC35	Strategic Communications	3	Credit
EC36	Information Security Policies	3	Credit
EC37	Introductory Practice	3	Credit
EC38	Industrial Practice	6	Credit
EC39	Pre-Diploma Practice	6	Credit
EC40	Qualification Work	6	Credit
Total volume of mandatory components:		**180**	
Elective Components of the Educational Program			
EC41	Student-Selected Component	5	Credit
EC42	Student-Selected Component	5	Credit
EC43	Student-Selected Component	5	Credit
EC44	Student-Selected Component	5	Credit
EC45	Student-Selected Component	5	Credit
EC46	Student-Selected Component	5	Credit
EC47	Student-Selected Component	5	Credit
EC48	Student-Selected Component	5	Credit
EC49	Student-Selected Component	5	Credit
EC50	Student-Selected Component	5	Credit
EC51	Student-Selected Component	5	Credit
EC52	Student-Selected Component	5	Credit
Total volume of elective components:		**60**	
TOTAL VOLUME OF THE EDUCATIONAL PROGRAM		**240**	

2.3. Structural-Logical Scheme of the Educational Program



Cycle of General Education Components	Student-Selected Components
Cycle of Professional and Practical Training Components	PRACTICE

3. Form of Assessment of Higher Education Students

Forms of assessment of higher education students	Assessment of higher education students is carried out in the form of a Unified State Qualification Examination and a public defense of the bachelor's qualification work.
Requirements for the Unified State Qualification Examination:	The Unified State Qualification Examination provides for the assessment of learning outcomes defined by this standard.
Requirements for the qualification work	The bachelor's qualification work involves solving a specialized task in the field of cybersecurity and information protection. The qualification work must not contain academic plagiarism, fabrication, or falsification. Plagiarism is checked in accordance with the Code of Academic Integrity of the State University of Information and Communication Technologies, enacted by the Rector's order dated August 14, 2023, № 111. The qualification work is published on the official website (or repository) of the State University of Information and Communication Technologies. Assessment is conducted openly and publicly.

4. Matrix of Alignment of Program Competencies with Educational Program Components

Educational Components	Competencies																		
	General Competencies									Special (Professional) Competencies									
	IC	GC 1	GC 2	GC 3	GC 4	GC 5	GC 6	GC 7	GC 8	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
EC.01	+					+													
EC.02	+						+			+	+	+							
EC.03	+	+	+																
EC.04	+			+															
EC.05	+				+														
EC.06	+			+															
EC.07	+	+	+				+	+											
EC.08	+		+				+	+	+										
EC.09	+						+			+									
EC.10	+								+										
EC.11	+	+							+										
EC.12	+		+						+										
EC.13							+		+										
EC.14	+	+	+			+												+	
EC.15	+	+	+			+													
EC.16	+						+			+									
EC.17	+			+					+		+								
EC.18	+																		+
EC.19	+										+		+						
EC.20	+	+							+								+		
EC.21	+										+								
EC.22	+														+			+	
EC.23	+	+	+								+								
EC.24	+		+				+	+		+									
EC.25	+		+				+	+		+									
EC.26	+											+				+			
EC.27	+															+			
EC.28	+															+			
EC.29	+										+			+					
EC.30	+											+							
EC.31	+										+			+					
EC.32	+											+	+						
EC.33	+	+			+		+	+											
EC.34	+																		+
EC.35	+	+	+		+					+									
EC.36	+									+		+				+			
EC.37	+	+	+				+		+	+	+								
EC.38	+	+	+			+	+	+	+	+	+	+							
EC.39	+	+	+			+	+	+	+	+	+	+	+	+					
EC.40	+	+	+			+	+	+	+	+	+	+	+	+		+			+

5. Matrix of Mapping Program Learning Outcomes (PLO) to the Corresponding Educational Program Components

Educational Components	Learning Outcomes																				
	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6	PLO 7	PLO 8	PLO 9	PLO 10	PLO 11	PLO 12	PLO 13	PLO 14	PLO 15	PLO 16	PLO 17	PLO 18	PLO 19	PLO 20	PLO 21
EC.01								+													
EC.02									+	+	+										
EC.03				+																	
EC.04	+																				
EC.05		+																			
EC.06	+																				
EC.07			+	+																	
EC.08			+			+															
EC.09									+												
EC.10								+													
EC.11							+														
EC.12		+				+															
EC.13			+			+			+												
EC.14					+			+												+	
EC.15					+			+													
EC.16									+												
EC.17						+				+											
EC.18																					+
EC.19										+		+	+								
EC.20							+											+	+		
EC.21										+											
EC.22																+				+	
EC.23					+					+											
EC.24			+	+	+				+												
EC.25			+	+	+				+												
EC.26		+									+						+				
EC.27																	+				
EC.28																	+				
EC.29										+				+	+						
EC.30											+										
EC.31										+		+	+								
EC.32											+	+	+								
EC.33	+	+	+																		
EC.34																					+
EC.35		+		+					+												
EC.36									+		+						+				
EC.37				+		+			+	+											
EC.38			+	+		+	+	+	+	+	+										
EC.39			+	+		+	+	+	+	+	+	+	+	+	+						
EC.40			+	+		+	+	+	+	+	+	+	+	+	+		+				+

Guarantor of the Educational Program
Associate Professor of the Department of Cybersecurity
and Information Protection Management
of the Educational-Scientific Institute of Cyber security and Information Protection
State University of Information and Communication Technologies

Candidate of Technical Sciences Dmytro RABCHUN