3. Educational program

Head of the project team (guarantor of the educational program) –
Savchenko T.V. Candidate of Technical Sciences, Associate Professor.

1. Profile of the educational program
from the specialty 125 " Cybersecurity "
(specialization "Security of information and communication systems in the economy")

1 – General information	
Full name of the higher educational establishment and structural unit	Kyiv National University of Trade and Economics Faculty of Information Technologies Department of Software Engineering and Cybersecurity
Degree of higher education and the name of the qualification in the language of the original	The degree of higher education «bachelor» specialty "Cybersecurity" specialization "Security of information and communication systems in the economy"
The official name of the educational program	"Security of information and communication systems in the economy"
Type of diploma and the volume of the educational program	Bachelor's degree, unitary 240 ECTS credits term of training 3 years and 10 months
Availability of accreditation	–
Cycle / Level	NQF of Ukraine – 6th level, FQ-EHEA – first cycle, EQF-LLL – 6th level
Prerequisites	Complete general secondary education, initial level of higher education
Language(s) of teaching	Ukrainian
The validity of the educational program	Until next scheduled update
Internet address of the permanent placement of the educational program	https://knute.edu.ua
2 - The purpose of the educational program	
Formation of a modern system of professional knowledge and skills in the field of security of information and communication systems of the enterprise (organization), *particular in the economy*. Formation of a person capable on the basis of acquired integrated, general and professional competencies to work successfully in the field of IT technologies, ensuring the security of information and communication systems of the enterprise (organization), *particular in the economy*	
3 – Characteristics of the educational program	
Subject area (branch of knowledge, specialty, specialization (if available))	Branch of knowledge 12 «Information technology Specialty 125 «Cybersecurity» Specialization «Security of information and communication systems in the economy»

The educational program orientation	Educational and professional. Aimed at training specialists combining fundamental mathematical, informational and economic positions with practical skills in the field of cybersecurity and information technology, using algorithms, methods and software development technology and cryptographic methods of information protection.
The main focus of the educational program and specialization	Special. Higher education in the subject area 125 "Cybersecurity" in branch of knowledge of information technology. Ability to organize and maintain a set of measures to ensure the security of information systems and networks of the enterprise (organization), taking into account their legal and economic feasibility, technical implementation, to avoid possible external influences, possible threats and the use of information security technologies. Keywords: security of information and telecommunication systems; cryptographic methods of information protection; number theory; security of operating systems and networks.
Features of the program	The program creates the following chain: tasks, knowledge, skills, abilities, professional activity, professional context, work area, interests, professional styles, professional values, related professions, salary. The modular principle is used to reveal the essence of the listed components. Integration of software and hardware for detecting, monitoring and providing IS, information technology information protection in information and communication systems of the enterprise, in particular in the economy, data storage technologies in a single information space and the introduction of cybercrime countermeasures.
4 - Eligibility of graduates for employment and further training	
Eligibility for employment	The specialist can hold primary positions (according to the Classifier of Professions of Ukraine DK 003: 2010): 3439 (24771). Information security specialist. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT). Can hold the following positions: - manager (manager) of information security systems (1495); - information security specialist (3439); *- specialist (field of information protection);* *- specialist in secrecy;* *- inspector for the organization of protection of classified information;* *- analyst of cybersecurity systems;* *- specialist in organizing and conducting penetration testing.*
Further education	Training according to the master's program of the 7th level of NRC of Ukraine, the second cycle of FQ-EHEA and the 7th level of EQF-LLL.
5 – Teaching and evaluation	
Teaching and learning	Student-centered learning, self-study, learning through laboratory practice, problem-based, interactive, design, information-computer, self-developing, collective and integrative, contextual learning technologies.

Evaluation	Evaluation is carried out according to the "Regulations on the assessment of learning outcomes of students and graduate students" and "Regulations on the organization of the educational process of students." **Types of control** over the levels: self-control, control at the level of the teacher, control at the level of the head of the department, control at the level of the dean's office, control at the level of the director, certification; **Control forms**: oral and written surveys, testing, presentation of scientific work, protection of coursework. Current control, final control - exams and tests, defense of the final qualification project.
6 – Program competencies	
Integral competence	Ability to solve complex specialized problems and practical problems in the field of information security and / or cyber security, in *particular in an economy* characterized by complexity and incomplete uncertainty of conditions.
General competences (GC)[1]	**GC 1**. Ability to apply knowledge in practical situations. **GC 2.** Knowledge and understanding of the subject area and understanding of the profession. **GC 3.** Ability to communicate professionally in state and foreign languages both orally and in writing. **GC 4.** Ability to identify, pose and solve problems in a professional direction. **GC 5.** Ability to search, process and analyze information. **GC 6.** Ability to exercise their rights and responsibilities as a member of society, to realize the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine. **GC 7**. Ability to preserve and increase moral, cultural, scientific values and achievements of society based on understanding the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, techniques and technologies, use different types and forms physical activity for active recreation and a healthy lifestyle. **GC 8**. *Basic knowledge of the basics of economics and entrepreneurship*.
Professional competence of the specialty (PC) [2]	**PC 1.** Ability to apply legal and regulatory framework as well as national and international requirements and standards of practice for the purpose of professional activities in the field of information security and / or cybersecurity. **PC 2**. Ability to use information and communication technologies, modern methods and models of information security and / or cybersecurity. **PC 3.** Ability to use software and software-hardware complexes of information security in information-telecommunication (automated) systems. **PC 4.** Ability to ensure business continuity in accordance with established information and / or cybersecurity policies.

	PC 5. The ability to protect information processed in information and telecommunication (automated) systems to implement the established policy of information and / or cybersecurity. **PC 6**. Ability to restore regular operation of information, information and telecommunication (automated) systems after the implementation of the threats, the implementation of cyber-attacks, crashes and failures of different classes and backgrounds. **PC 7**. Ability to establish and ensure the functioning of complex information security systems (complex legal, organizational and technical means and methods, procedures, practical techniques and so on.). **PC 8.** Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. **PC 9.** Ability to carry out professional activities on the basis of the implemented information and / or cyber security management system. **PC 10**. Ability to apply methods and means of cryptographic and technical protection of information on the objects of information activities. **PC 11.** Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and / or cybersecurity. **PC 12.** Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and / or cybersecurity policies. ***PC 13****. Ability to conduct technical and economic analysis and substantiate design decisions to ensure cybersecurity.* ***PC 14.*** *Ability to manage information and cybersecurity risks.*
7 – Program learning outcomes(PLO)[1]	
	1. Apply knowledge of state and foreign languages in order to ensure the efficiency of professional communication. **2.** To organize own professional activity, to choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, to estimate their efficiency. **3.** Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of problems of specialized professional activities. **4.** Analyze, argue, make decisions in solving complex specialized problems and practical problems in professional activities, which are characterized by complexity and incomplete definition of conditions, be responsible for decisions. **5.** To adapt in the conditions of frequent change of technologies of professional activity, to predict the final result.

[3] *The program learning outcomes determined by the graduating department are highlighted in italics.*

	6. Critically comprehend the basic theories, principles, methods and concepts in teaching and professional activities. **7.** Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and / or cybersecurity. **8.** Prepare proposals for regulations to ensure information and / or cybersecurity. **9**. Implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents. **10.** Perform analysis and decomposition of information-telecommunication systems. **11.** Perform analysis of relationships between information processes on remote computing systems. **12**. Develop model threats and offender. **13.** Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols. **14.** Solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and evaluate the effectiveness of the quality of decisions**.** **15.** Use modern software and hardware information and communication technologies. **16.** To implement comprehensive information security system in automated systems (AS) organization (company) in accordance with the requirements of regulatory documents. **17.** To provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge, concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interconnections. languages and information flows, processes for internal and remote components. **18.** Use software and firmware systems to protect information resources. **19.** Apply theories and methods of protection to ensure information **20**. Ensure the operation of special software to protect information from destructive software influences, destructive codes in information and telecommunications systems. **21.** Solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information and information and telecommunications (automated) systems. **22**. Solve the tasks of managing the procedures of identification, authentication, authorization of processes and users in information and telecommunication systems in accordance with the established policy of information and / or cybersecurity. **23**. Implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems. **24**. Solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role).

	25. Ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information-telecommunication (automated) systems using event logs, their analysis and established protection procedures. **26.** Implement measures and ensure the implementation of processes to prevent unauthorized access and protection of information, information and telecommunications (automated) systems based on the reference model of interaction of open systems. **27**. Solve problems of data flow protection in information, information and telecommunication (automated) systems. **28**. Analyze and assess the effectiveness and level of protection of resources of different classes in information and information and telecommunications (automated) systems during testing in accordance with the established policy of information and / or cybersecurity. **29**. To assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes. **30**. Assess the possibility of unauthorized access to elements of information and telecommunications systems. **31**. Apply theories and methods of protection to ensure the security of elements of information and telecommunications systems. **32**. To solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy. **33**. Solve the problem of ensuring continuity of business processes of the organization based on the theory of risk **34**. Participate in developing and implementing strategies informational safety and / or cyber security in accordance with the goals and objectives of the organization. **35**. Solve the problem of providing and maintaining comprehensive information security systems, as well as counteracting unauthorized access to information resources and processes in information and information and telecommunications (automated) systems in accordance with the established policy of information and / or cybersecurity. **36**. Detect dangerous signals of technical means. **37**. Measure the parameters of dangerous and interference signals during the instrumental control of information protection processes and determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulations of the technical information protection system. **38**. Interpret the results of special measurements using technical means, control the characteristics of information and telecommunications systems in accordance with the requirements of regulatory documents of the technical protection of information. **39.** Carry out the certification (based on registration and inspection) of regime territories (zones), premises, etc. in the conditions of observance of the regime of secrecy with recording of results in the relevant documents. **40**. Interpret the results of special measurements using technical means, control the characteristics of ITS in accordance with the requirements of

	41. Ensure continuity of the process of keeping logs of events and incidents on the basis of automated procedures. **42**. Implement processes of detection, identification, analysis and incident response information and / or cybersecurity. **43**. Use national and international regulatory acts in the field of information security and / or to investigate cyber security incidents. **44**. Solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards. **45**. Apply different classes of information security and / or cybersecurity policies based on risk-based control of access to information assets. **46**. Analyze and minimize the risks of information processing in information and telecommunications systems. **47**. To solve problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information. **48**. To perform implementation and support of intrusion detection systems and components using encryption to ensure the necessary protection of information in telecommunication systems. **49**. To ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunications systems. **50**. To ensure the functioning of software and hardware systems for detecting intrusions of different levels and classes (statistical, signature, statistical-signature). **51**. To maintain efficiency and ensure the configuration of intrusion detection in information and telecommunication systems. **52**. To use tools for monitoring processes in information and telecommunication systems. **53**. To solve the problem of analyzing the program code for possible threats. **54**. To aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine. ***55. To analyze the cost-effectiveness of information security measures.*** ***56. To apply knowledge of methods of technical and economic analysis and justification of design decisions.***

8 – Resource support for the implementation of the program	
Personnel provision	Project team: 3 doctors of sciences and 6 candidates of sciences. All developers are employees of the Kyiv National University of Trade and Economics. Scientific and pedagogical workers with scientific degrees and / or academic titles, as well as highly qualified specialists are involved in the implementation of the program. In order to improve the professional level, all scientific and pedagogical staff are trained once every five years.
Material and technical support educational	Special computer labs with modern hardware and software resources form the basis of material and technical security, which provide quality training for bachelors in the educational program "Security of information and communication systems in the economy."
Informational and educational support	MOODLE's learning system and MS Office 365 environment allow students to work independently and individually
9 – Academic mobility	
National credit mobility	Organization of credit mobility (except for the 1st year) of students who obtain a bachelor's degree. Project EPAM Systems Ukraine, Ukrainian Institute of Intellectual Property, Procom Certified Training Center, Pearson Education Educational Company, Parus Corporation, BGS Solutions Group of Companies.
International credit mobility	Organization of credit mobility (except for the 1st year) of bachelors. Project Paris Est Creteil University (Paris, France), Audencia Business School (Nantes, France, University of Grenoble Alps (Grenoble, France), University of Central Lancashire (Preston, UK), Hohenheim University (Stuttgart, Germany).
Education for foreign applicants for higher education	Conditions and features of the educational program in the context of teaching foreign citizens: knowledge of the Ukrainian language at a level not lower than B1.

2. List of components of the educational program and their logical consistency

2.1. List of components of EP

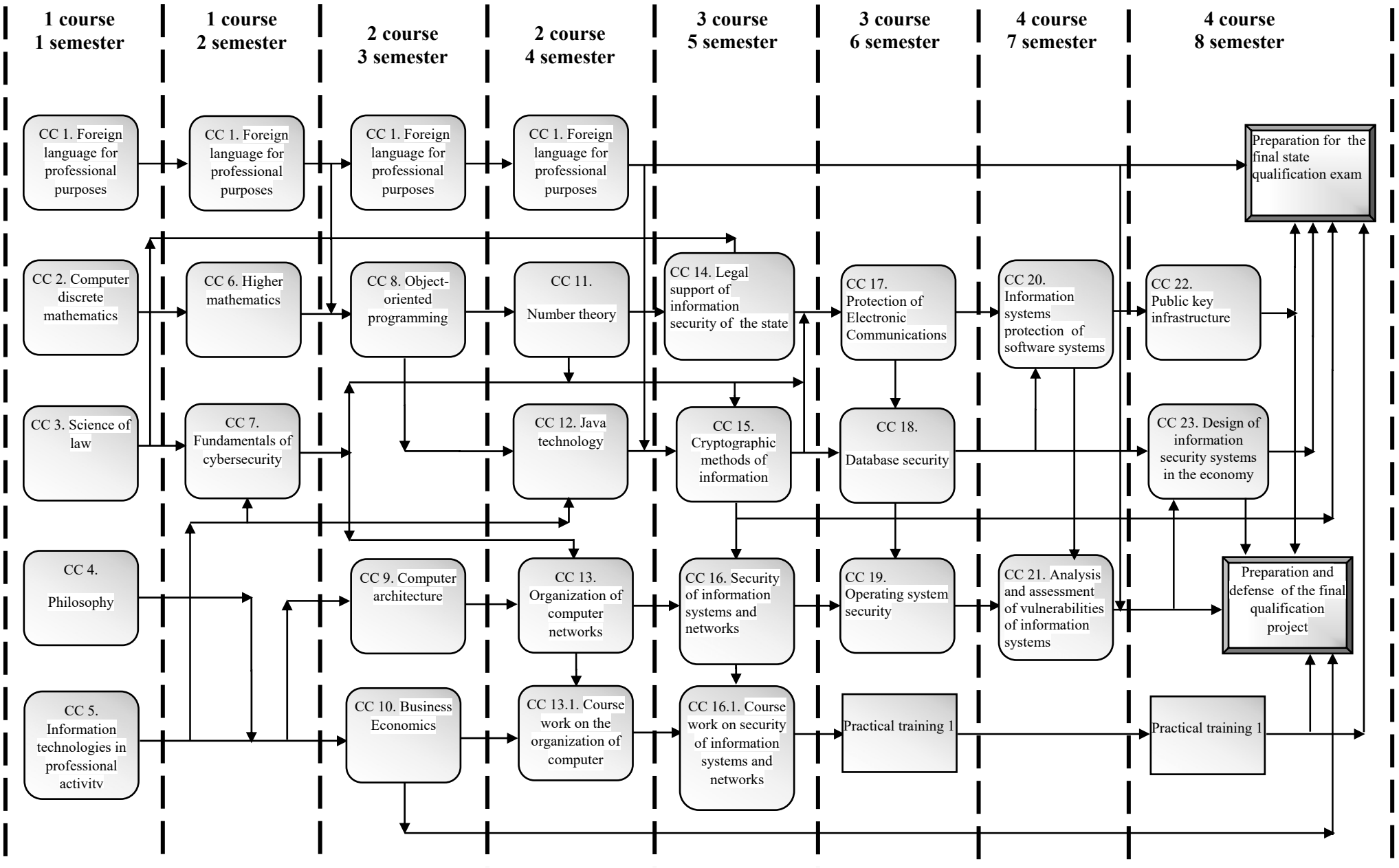
Code e/d	Components of the educational program (educational disciplines, term papers), field experience, final qualification work)	Number of credits
1	2	3
1. Compulsory Components of EP		
CC 1.	Foreign language for professional purposes	24
CC 2.	Computer discrete mathematics	6
CC 3.	Science of law	6
CC 4.	Philosophy	6
CC 5.	Information technologies in professional activity	6
CC6	Higher mathematics	6
CC 7.	Fundamentals of cybersecurity	6
CC 8.	Object-oriented programming	6
CC 9.	Computer architecture	6
CC 10.	Business Economics	6
CC 11.	Number theory	6
CC12	Java technology	6
CC 13.	Organization of computer networks	6
CC 13.1.	Course work on the organization of computer networks	
CC 14.	Legal support of information security of the state	6
CC 15.	Cryptographic methods of information protection	6
CC 16.	Security of information systems and networks	6
CC 16.1.	Course work on security of information systems and networks	
CC 17.	Protection of Electronic Communications	6
CC 18.	Database security	6
CC 19.	Operating system security	6
CC 20.	Software systems for information systems protection	6
CC 21.	Analysis and assessment of vulnerabilities of information systems	6
CC 22.	Public key infrastructure	7,5
CC 23.	Design of information security systems in the economy	7,5
The total amount of Compulsory Components:		**159**

1	2	3
2. Selective components of EP		
SC 1	Algorithms and data structures	6
SC 2	Software architecture and design	6
SC 3	Life safety	6
SC 4	Diplomatic and business protocol and etiquette	6
SC 5	Contract law	6
SC 6	Expert systems	6
SC 7	Electronic document management	6
SC 8	Investment law	6
SC 9	Business analytics tools	6
SC 10	Information law	6
SC 11	History of Ukraine	6
SC 12	History of Ukrainian Culture	6
SC 13	Computer graphics and data visualization	6
SC 14	Logics	6
SC 15	Human-machine interaction	6
SC 16	Mathematical programming	6
SC 17	Software project management	6
SC 18	Methods and means of data transmission	6
SC 19	International Economics	6
SC 20	Data models and structures	6
SC 21	Modeling of economic processes	6
SC 22	Software modeling and analysis	6
SC 23	National interests in world geopolitics and geoeconomics	6
SC 24	Basics of programming	6
SC 25	Politology	6
SC 26	EU law	6
SC 27	Internet programming	6
SC 28	Design and administration of information systems	6
SC 29	Security psychology	6
SC 30	Labor psychology and engineering psychology	6
SC 31	Management psychology	6
SC 32	Psychology	6
SC 33	Religious studies	6

SC 34	World culture	6
SC 35	Data analysis technology	6
SC 36	Software development and testing technology	6
SC 37	Startup technology	6
SC 38	Ukrainian language (for professional purposes)	6
SC 39	Informatization project management	6
SC 40	Artificial Intelligence	6
SC 41	WEB-design and WEB-programming	6
The total amount of Selective components:		**60**
3. Practical studying		
Internship (Industrial practice) 1		6
Internship (Industrial practice) 2		6
The total		**12**
4. Attestation		
Preparation for certification		3
Preparation of the final qualification project and defense		6
The total		**9**
THE TOTAL VOLUME OF EDUCATIONAL PROGRAM		**240**

For all components of the educational program, the form of final control is an exam.

2. 2. Structural and logical scheme of EP



3. The form of certification of higher education applicants

Certification of graduates is carried out in the form of public defense of the final qualification project.

A set of knowledge, skills, abilities and other competencies acquired by a person in the process of studying according to the standard of higher education is submitted for certification.

Students who have fulfilled all the requirements of the training program are admitted to the certification.

The final qualification project should address a specialized problem in the field of information and / or cybersecurity, in particular in economics.

The final qualification project must be tested for plagiarism.

The final qualification project must be published on the official website of the KNTEU institution or its subdivision, or in the repository of the higher education institution.

4.1. Matrix of correspondence of program competences compulsory components of the educational program

Components / competences	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10	CC 11	CC 12	CC 13	CC 14	CC 15	CC 16	CC 17	CC 18	CC 19	CC 20	CC 21	CC 22	CC 23
GC 1	+	+			+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+
GC 2							+	+	+				+		+		+			+	+		+
GC 3	+																						
GC 4							+								+	+		+	+	+	+		+
GC 5		+			+	+					+		+			+		+	+				
GC 6			+											+									
GC 7			+	+						+		+		+									
GC 8										+													
PC 1			+											+								+	
PC 2		+			+		+	+									+			+			
PC 3									+			+					+			+			
PC 4							+																
PC 5		+														+	+	+	+	+			
PC 6													+				+			+			
PC 7							+							+						+			+
PC 8							+														+		
PC 9							+														+		
PC 10							+								+							+	+
PC 11							+										+						
PC 12							+						+			+		+	+		+	+	+
PC 13					+																		+
PC 14										+											+		

4.2. Matrix of correspondence of program competences selective components of the educational program

Components / competences	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10	SC 11	SC 12	SC 13	SC 14	SC 15	SC 16	SC 17	SC 18	SC 19	SC 20	SC 21	SC 22	SC 23	SC 24	SC 25	SC 26	SC 27	SC 28	SC 29	SC 30	SC 31	SC 32	SC 33	SC 34	SC 35	SC 36	SC 37	SC 38	SC 39	SC 40	SC 41
GC 1	+	+		+	+	+	+	+	+	+			+	+	+	+			+	+	+	+	+	+		+	+	+	+	+	+		+		+	+	+		+	+	+
GC 2		+					+								+		+	+		+	+	+		+			+	+							+		+				
GC 3																																						+			+
GC 4	+	+				+			+						+	+	+			+	+	+		+			+	+				+			+				+	+	
GC 5	+			+		+	+		+				+	+	+	+	+	+	+	+	+	+	+	+			+	+							+				+	+	
GC 6				+	+			+		+	+	+							+				+		+	+			+	+	+	+		+						
GC 7			+	+							+	+							+				+		+								+	+		+					
GC 8																			+																						
PC 1					+			+		+																+			+	+	+										
PC 2	+					+										+		+		+	+	+		+				+							+					+	
PC 3																								+				+							+						
PC 4									+								+																						+		+
PC 5																																									
PC 6																																									
PC 7																																									
PC 8						+			+									+																	+				+	+	
PC 9							+																																		
PC 10																		+																							
PC 11		+				+									+					+	+	+																	+	
PC 12						+								+											+		+					+			+				+	
PC 13																																									
PC 14																																									

5.1. Matrix for providing software learning outcomes relevant compulsory components of the educational program

Components Program learning outcomes	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10	CC 11	CC 12	CC 13	CC 14	CC 15	CC 16	CC 17	CC 18	CC 19	CC 20	CC 21	CC 22	CC 23
1	+																						
2						+					+												
3				+				+			+	+											
4				+							+												
5					+			+				+											
6							+																
7			+											+								+	
8			+											+								+	
9			+											+							+	+	
10					+				+		+												
11					+				+			+											
12													+										+
13													+								+		
14									+							+	+	+	+				
15									+														+
16																+	+	+	+			+	
17																+	+	+	+				+
18									+											+			
19							+									+	+	+	+				
20									+							+	+	+	+	+			
21								+				+				+	+	+	+		+		
22		+																					
23							+																
24							+																
25							+																
26													+							+			+
27																+	+	+	+				
28																+	+	+	+		+		

5.1. Matrix for providing software learning outcomes relevant compulsory components of the educational program (continued)

Components / Program learning outcomes	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10	CC 11	CC 12	CC 13	CC 14	CC 15	CC 16	CC 17	CC 18	CC 19	CC 20	CC 21	CC 22	CC 23
29							+																
30							+													+			
31							+																
32							+																
33							+				+												
34																+	+	+	+				+
35							+													+			
36																				+			
37																+	+	+	+				
38																	+				+		
39														+									
40														+						+			
41																		+					
42							+													+	+		+
43														+									
44							+															+	
45														+									
46					+																+		
47							+								+						+		+
48													+		+						+		+
49																	+						
50									+											+			+
51									+											+			
52																					+		
53		+																					
54			+	+																			
55										+													+
56					+																		+

5.2. Matrix for providing software learning outcomes relevant elective components of the educational program

Components / Program learning outcome	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10	SC 11	SC 12	SC 13	SC 14	SC 15	SC 16	SC 17	SC 18	SC 19	SC 20	SC 21	SC 22	SC 23	SC 24	SC 25	SC 26	SC 27	SC 28	SC 29	SC 30	SC 31	SC 32	SC 33	SC 34	SC 35	SC 36	SC 37	SC 38	SC 39	SC 40	SC 41
1																																					+			
2				+									+				+		+				+					+			+				+		+			
3				+					+				+	+			+		+		+	+	+	+			+	+					+	+	+					
4				+					+							+			+		+	+	+					+								+			+		
5																	+							+			+	+		+										+	
6				+									+						+				+	+				+			+		+		+						
7					+		+	+		+									+				+			+															
8					+			+		+																+															
9										+									+				+						+	+	+			+							
10	+								+									+				+						+													
11									+						+																				+			+			
12																				+	+	+																			
13									+						+			+																			+		+		
14		+					+		+													+																			
15		+					+		+									+																						+	
16					+		+	+	+	+																+													+		
17	+	+																		+		+														+						
18		+																																								
19																		+																		+						
20																		+				+																			
21																	+																									
22																	+																							+		
23						+																							+											+	
24																	+											+			+								+		
25			+																										+	+	+										
26						+																							+											+	
27	+																			+																+						
28																	+				+																		+			

5.2. Matrix for providing software learning outcomes relevant elective components of the educational program (continued)

Components /Program learning outcomes	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10	SC 11	SC 12	SC 13	SC 14	SC 15	SC 16	SC 17	SC 18	SC 19	SC 20	SC 21	SC 22	SC 23	SC 24	SC 25	SC 26	SC 27	SC 28	SC 29	SC 30	SC 31	SC 32	SC 33	SC 34	SC 35	SC 36	SC 37	SC 38	SC 39	SC 40-	SC 41
29						+																																	+	
30						+																																	+	
31																		+																						
32						+																																	+	
33																	+																						+	
34									+																															
35						+																																	+	
36																		+																	+	+				
37																																								
38																																								
39			+																																				
40																																								
41																	+													+									+	
42									+																										+					
43					+			+		+																+														
44									+								+																						+	
45																	+																						+	
46						+			+																															+	
47																+					+																			
48																+					+																			
49									+								+																			+			+	
50		+																																						
51						+																																	+	
52									+																											+				
53		+				+										+																							+	
54					+			+		+	+	+													+	+			+	+	+	+								
55																																								
56																																								