3. Educational programme

Director of the Bachelor's degree programmeme – T.O. Zhirova, PhD in Pedagogics, Associate Professor.

Head of the project team – Savchenko T.V. PhD in Engineering, Associate Professor.

1. Profile of the educational programme "Security of information and communication systems in the economy" from the Subject Area 125 " Cybersecurity and information protection"

1 - General information	
Full name of the higher educational establishment and structural unit	National University of Trade and Economics Faculty of Information Technologies Department of Software Engineering and Cybersecurity
Academic Degree and the name of the qualification in the language of the	The degree of higher education «bachelor» Subject Area "Cybersecurity and information protection "
The official name of the educational programme	"Security of information and communication systems in the economy"
Compliance with the standard of higher education of the Ministry of Education and Science of Ukraine	The SHE of the MEC of Ukraine is in charge
Type of diploma and the volume of the educational programme	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 (Short) Cycle
Мова(и) викладання	Ukrainian
Термін дії освітньої програми	Until next scheduled update
Інтернет - адреса постійного розміщення опису освітньої	https://knute.edu.ua
2 - The purpose of the educational programme	
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 programme	
Subject area	*Objects of professional activity of graduates:* - informatization objects, including computer, automated, telecommunication, information, information-analytical, information-telecommunication systems, information resources and technologies; – technologies for ensuring information security; – processes of information and/or cyber security management of objects to be protected. *The purpose of the training* is to prepare specialists who are able to use and implement information and/or cyber security technologies. *The theoretical content of the subject area* *Knowledge* – the legislative, regulatory and legal framework of Ukraine and the requirements of relevant international standards and practices regarding professional activity; – principles of supporting systems and complexes of information and/or cyber security; – theories, models and principles of managing access to information resources; – theories of information and/or cyber security management systems; – methods and means of identifying, managing and identifying risks; – methods and means of assessment and ensuring the required level of information security; – methods and means of technical and cryptographic protection of information; – modern information and communication technologies; – modern hardware and software of information and communication technologies; – automated design systems. *Methods, methodologies and technologies:* Methods, techniques, information and communication technologies and other technologies for ensuring information and/or cyber security. *Instruments and equipment:* – systems for developing, ensuring, monitoring and controlling information and/or cyber security processes; - modern software and hardware support of information and communication technologies.
The educational programme orientation	Educational-professional. It is aimed at training specialists who combine fundamental mathematical, information and economic principles with practical skills in the field of cyber security and information technologies, applying algorithms, methods and technologies of software development and cryptographic methods of information protection.

The main focus of the educational programme and specialization	Special. Higher education in the Subject Area 125 "Cyber security and information protection" in the field of information technologies. The 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 justification, technical implementation, prevention of possible external influences, probable threats and the application of information protection technologies. Keywords: security of information and telecommunication systems; cryptographic methods of information protection; number theory; security of operating systems and networks.
Features of the programme	The programme 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. The integration of software and hardware for detecting, monitoring and information security, information technology for information protection in information and communication systems of the enterprise, particularly in the economy, data storage technologies in a single information space and the implementation 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 the confidentiality regime;* – *inspector for the organization of protection of secret information;* – *analyst of cyber security systems;* – *specialist in the organization and conduct of penetration testing*
Further education	Training according to the master's programme of the 7th level of NRC of Ukraine, the second cycle of FQ-EHEA and the 7th level of EQF-LLL.
5 - Teaching and Assessment	
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.

Assessment	Assessment 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, defence of coursework. Current control, final control - exams and defense of the unified state qualifying exam
6 - Programme competences	
Integral competence	The ability to solve complex specialized tasks and practical problems in the field of information security, *in particular, in the economy,* which is characterized by complexity and incomplete determination of conditions.
General competences (GC)[1]	**GC** 1. Abilities to apply knowledge in practical situations. **GC**2. Knowledge and understanding of the subject area and understanding of the profession. **GC**3. Abilities to communicate professionally in state and foreign languages, both orally and in writing. **GC**4. Abilities to identify, pose and solve problems in a professional direction. **GC** 5. Abilities to search, process and analyze information. **GC** 6. Abilities 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. Abilities to preserve and multiply 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.** Abilities 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.** Abilities to use information and communication technologies, modern methods and models of information security and / or cybersecurity. **PC 3**. Abilities to use software and software-hardware complexes of information security in information-telecommunication (automated) systems. **PC 4.** Abilities to ensure business continuity in accordance with established information and / or cybersecurity policies.

Professional competence of the specialty (PC)[1]	**PC 1.** Abilities 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**. Abilities to use information and communication technologies, modern methods and models of information security and / or cybersecurity. **PC 3**. Abilities to use software and software-hardware complexes of information security in information-telecommunication (automated) systems. **PC 4.** Abilities to ensure business continuity in accordance with established information and / or cybersecurity policies. **PC 5.** Abilities to protect information processed in information and telecommunication (automated) systems to implement the established policy of information and / or cybersecurity. **PC 6.** Abilities to restore regular operation of information, information and telecommunication (automated) systems after the implementation of the threats, the implementation of cyberattacks, crashes and failures of different classes and backgrounds. **PC 7.** Abilities to establish and ensure the functioning of complex information security systems (complex legal, organizational and technical means and methods, procedures, practical techniques and etc.) **PC 8.** Abilities to carry out incident management procedures, conduct investigations, provide them with an assessment. **PC 9.** Abilities to carry out professional activities on the basis of the implemented information and / or cyber security management system. **PC 10**. Abilities to apply methods and means of cryptographic and technical protection of information on the objects of information activities. **PC 11**. Abilities to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and / or cybersecurity. **PC 12**. Abilities 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.*** *Abilities to conduct technical and economic analysis and substantiate design decisions to ensure cybersecurity.* ***PC 14.*** *Abilities to manage information and cybersecurity risks.*
7 - Programme 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 tasks 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 specialized professional activities. **4.** Analyze, argue, make decisions in solving complex specialized tasks 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. **6.** Critically comprehend the basic theories, principles, methods and concepts in studying 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 programmes 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 security in information and telecommunications systems.

	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 registration 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 in-formational 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 regulatory documents of the technical protection of information. **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 defence 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-hardware systems for detecting intrusions of different levels and classes (statistical, signature, statistical-signature). **51.** To maintain performance and ensure configuration of intrusion detection in information and telecommunication systems. **52.** To use tools for monitoring processes in information and telecommunication systems.

	53. Вирішувати задачі аналізу програмного коду на наявністьможливих загроз. **53.** To solve the problem of analyzing the programme 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 programme	
HR (Human resources)	Project team: 3 Doctors of Sciences and 6 PhD (candidates). All developers are employees of the 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 programme. 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 programme "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 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, corporation "Parus", group of companies "BGSSolutions".
International credit mobility	Organization of credit mobility (except 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 students	Conditions and features of the educational programme in the context of teaching foreign students: knowledge of the Ukrainian language at a level not lower than B1.

[1]General competences determined by the graduation department are highlighted in italics.
[2] Professional competences determined by the graduation department are highlighted in italics.

List of components of the educational programme and their logical consistency

2.1. List of components of EP

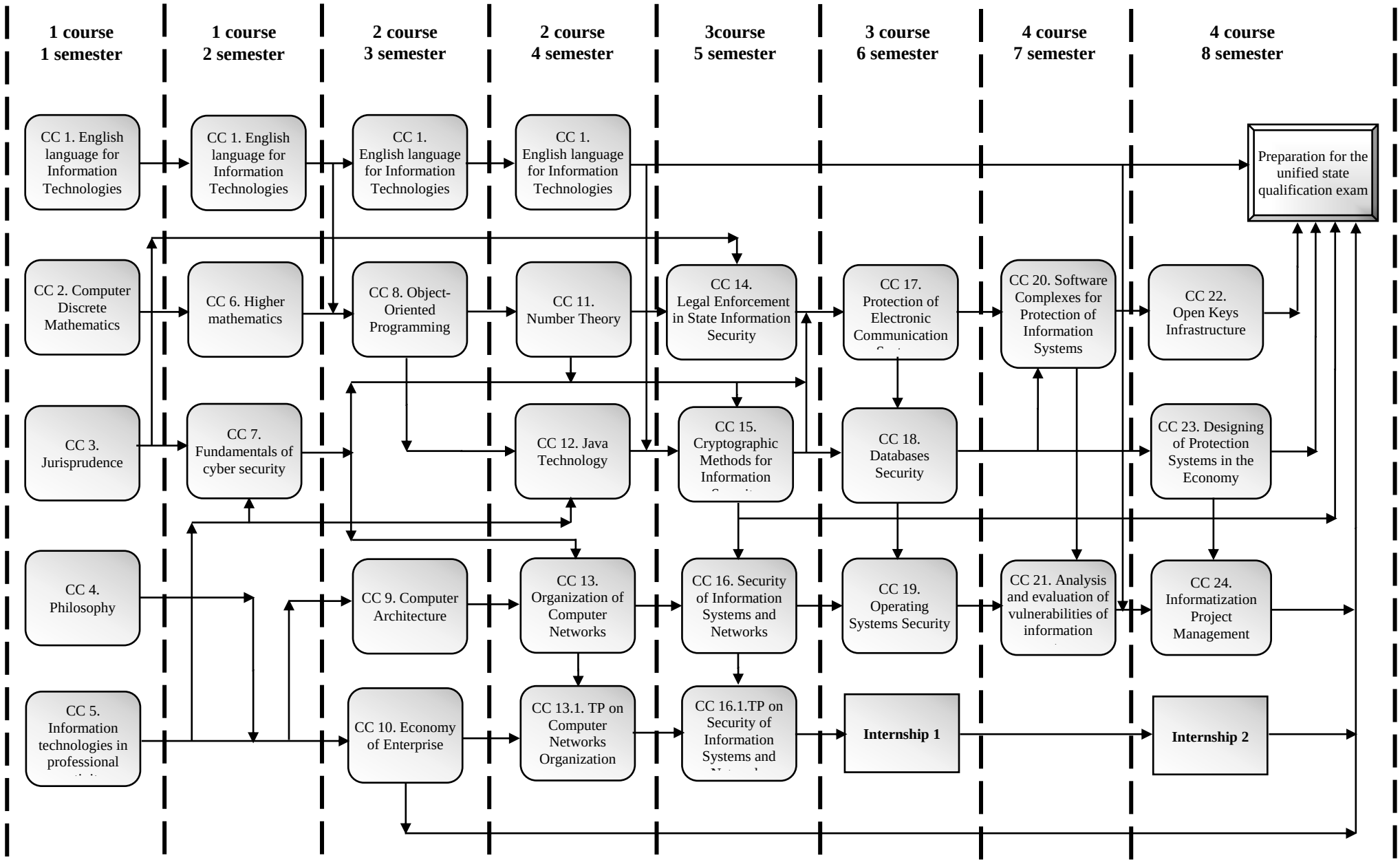
Code e/d	Components of the educational programme (educational disciplines, term papers), field experience, final qualification work)	Number of credits
1	2	3
1. Compulsory Components of EP		
CC 1.	English language for Information Technologies	24
CC 2.	Computer Discrete Mathematics	6
CC 3.	Jurisprudence	6
CC 4.	Philosophy	6
CC 5.	Information technologies in professional activity	6
CC 6.	Higher mathematics	6
CC 7.	Socio-technical cybersecurity	6
CC 8.	Object-Oriented Programmeming	6
CC 9.	Computer Architecture	6
CC 10.	Economy of Enterprise	6
CC 11.	Number Theory	6
CC 12.	Java Technology	6
CC 13.	Organization of Computer Networks	6
CC 13.1.	Term Paper on Computer Networks Organization	
CC 14.	Legal Enforcement in State Information Security	6
CC 15.	Cryptographic Methods for Information Security	6
CC 16.	Security of Information Systems and Networks	6
CC 16.1.	Term Paper on Security of Information Systems and Networks	
CC 17.	Protection of Electronic Communication Systems	6
CC 18.	Databases Security	6
CC 19.	Operating Systems Security	6
CC 20.	Software Complexes for Protection of Information Systems	6
CC 21.	Analysis and evaluation of vulnerabilities of information systems	6
CC 22.	Open Keys Infrastructure	7,5
CC 23.	Designing of Protection Systems in the Economy	7,5
CC 24.	Informatization Project Management	6
	Physical Education	
Total amount of Compulsory Components:		**165**

1	2	3
2. Optional components of EP		
1	2	3
OC 1.	Algorithms and Data Structures	6
OC 2.	Architecture and Software Design	6
OC 3.	Life Safety	6
OC 4.	Diplomatic and Business Protocol and Etiquette	6
OC 5.	Contract Law	6
OC 6.	Expert Systems	6
OC 7.	Electronic Documents Flow	6
OC 8.	Information Wars	6
OC 9.	Investment Law	6
OC 10.	Business Intelligence Tools	6
OC 11.	Information Law	6
OC 12.	History of Ukraine	6
OC 13.	History of Ukrainian Culture	6
OC 14.	Computer graphics and data visualisation	6
OC 15.	Logic	6
OC 16.	Human-machine Interaction	6
OC 17.	Mathematical Programmeming	6
OC 18.	Software Project Management	6
OC 19.	Data Transition Methods	6
OC 20.	International Economy	6
OC 21.	Data Models and Structures	6
OC 22.	Modelling of Bisness Processes	6
OC 23.	Software Modeling and Analysis	6
OC 24.	National Interests in World Geo-policy and Geo-economy	6
OC 25.	Fundamentals of programmeming	6
OC 26.	Political Science	6
OC 27.	EU Law	6
OC 28.	Internet Programmeming	6
OC 29.	Design and administration of information systems	6
OC 30.	Psychology of Security	6
OC 31.	Labor Psychology and Engineering Psychology	6
OC 32.	Management Psychology	6

ОС 33.	Psychology	6
ОС 34.	Religious Studies	6
ОС 35.	World Culture	6
ОС 36.	Data Analysis Technology	6
ОС 37.	Software Development and Testing Technology	6
ОС 38.	Startup Creation Technology	6
ОС 39.	Ukrainian Language (professional)	6
ОС 40.	Artificial Intelligence	6
ОС 41.	WEB-дизайн і WEB-програмування	6
Total amount of optional components:		**60**
3. Internship		
Industrial practice 1		6
Industrial practice 2		6
Total		**12**
4. Attestation		
Preparation for the unified state qualification exam		3
Total		**3**
TOTAL VOLUME OF EDUCATIONAL PROGRAMME		**240**

For all components of the educational programme, 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

Attestation is carried out in the form of a unified state qualification exam.

The unified state qualification exam provides for the assessment of the achievement of learning outcomes defined by this standard and the educational programme.

4.1. Matrix of suitability of programme competences compulsory components of the educational programme

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 suitability of programme competences optional components of the educational programme

Components / Competences	OC 1	OC 2	OC 3	OC 4	OC 5	OC 6	OC 7	OC 8	OC 9	OC 10	OC 11	OC 12	OC 13	OC 14	OC 15	OC 16	OC 17	OC 18	OC 19	OC 20	OC 21	OC 22	OC 23	OC 24	OC 25	OC 26	OC 27	OC 28	OC 29	OC 30	OC 31	OC 32	OC 33	OC 34	OC 35	OC 36	OC 37	OC 38	OC 39	OC 40	OC 41	OC 42	OC 43
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 of providing of programme learning outcomes appropriate compulsory components of the educational programme

Components/ Programme 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 of providing of programme learning outcomes appropriate compulsory components of the educational programme (continuation)

Components/ Programme 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 of providing of programme learning outcomes appropriat optional components of the educational programme

Components/ Programme learning outcomes	OC 1	OC 2	OC 3	OC 4	OC 5	OC 6	OC 7	OC 8	OC 9	OC 10	OC 11	OC 12	OC 13	OC 14	OC 15	OC 16	OC 17	OC 18	OC 19	OC 20	OC 21	OC 22	OC 23	OC 24	OC 25	OC 26	OC 27	OC 28	OC 29	OC 30	OC 31	OC 32	OC 33	OC 34	OC 35	OC 36	OC 37	OC 38	OC 39	OC 40	OC 41	OC 42	OC 43
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 of providing of programme learning outcomes appropriate optional components of the educational programme (continuation)

Components/ Programme 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	SC 42	SC 43
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																																												