BORYS GRINCHENKO KYIV UNIVERSITY

«APPROVED»

Decision of the Academic Council,
Borys Grinchenko Kyiv University

23 November 2017, Protocol No.11

The Head of the Academic Council, Rector
Viktor Ogneviuk

Programme of Study (Vocational)

125.00.01 Security of information and communication systems first (bachelor) level of higher education

Field of Knowledge:	**12 Information technology**
Specialty:	**125 Cybersecurity**
Qualifications**:**	**Bachelor of Cybersecurity**
	3439 Specialist in Information Security

Enacted since 01 September 2018
(Order No.762, November-24-2017)

Kyiv – 2017

LETTER OF APPROVAL
Programme of Study (Vocational)

The Chair of Information and Cybernetic Security of the Faculty of Information Technologies and Management Borys Grinchenko Kyiv University

Protocol No. ____, ___ _____ 2018

The Head of the Chair _____ Volodymyr Buriachok

The Academic Council of information and cybernetic security of the Faculty of information technologies and management Borys Grinchenko Kyiv University
Protocol No.___, ___ _____ 2018

The Head of the Academic Council _____ Alla Mykhatska

PREAMBLE

The programme of study (vocational) complies with the Law of Ukraine "On Higher Education", 01.07.2015, No.1556-VII, and the Draft of the Standard for Higher Education of Ukraine in the field of knowledge 125 Cybersecurity.

№ _____ ____ _____ 20

The programme of study (vocational) was developed by a working group consisting of:

The head of working group:
Viktor Semko, Doctor of Technical Sciences, Associate Professor, Professor of Information and Cybernetic Security Department, Boris Grinchenko Kyiv University

Working group members:
Anatoly Bessalov, Doctor of Technical Sciences, Professor, Professor of the Department of Information and Cybernetic Security of Kyiv Boris Grinchenko University

Iryna Melnyk, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information Technologies and Mathematical Disciplines of Kyiv Boris Grinchenko University

Valerii Yermoshyn, Candidate of Technical Sciences, Associate Professor of the Department of Information and Cybernetic Security of Kyiv Boris Grinchenko University (part-time)

External Reviewers:
Volodymyr Khoroshko, Doctor of Technical Sciences, Professor, Professor of the Department of Information Technology Security, Kyiv National Aviation University, Kyiv

Yanina Roy, Candidate of Technical Sciences, Information Security Analyst, SI Center Ltd, Kyiv

Educational and professional program is introduced for the first time

Term view of educational and vocational programs _____ in _____ years

Actualized:

Date of Review of the PS /Amendments to PS			
Signature:____			
Name of PS Guarantor			

I. PROFILE OF THE PROGRAMME OF STUDY (VOCATIONAL)

SOCIAL COMMUNICATIONS

1 - General information	
The full name of the higher education institution and the structural unit	Boris Grinchenko Kyiv University Faculty of information technologies and management
Degree of higher education	Bachelor
Educational qualification	Bachelor’s degree in Cyber Security, Specialist in Information Security
Official name of the programme of study	125.00.01 Security of Information and Communication Systems
Type of diploma and term of study according to the programme	240 credits ECTS Bachelor’s degree, unitary term of study: 3 year 10 months
Availability of accreditation	Implementation in 2018
Cycle / Level	First (bachelor) level / FQ-EHEA-first cycle, EQF LLL-6 level, HPK-7 level
Prerequisites	Complete General secondary education. Vocational education with Bachelor's or Junior Specialist's degree
Language (s) of teaching	Ukrainian
Validity of the programme of study	2023
Internet address of the permanent placement of the description of the programme of study	http://kubg.edu.ua/

2 - The purpose of the programme of study (vocational)
To provide students with high-quality theoretical and practical training in the form of knowledge and skills in the specialty 125 Cybersecurity for the organization and maintenance of information security at the objects of information activity

3 - Characteristics of the programme of study	
Subject area: 12 Information technology 125 Cybersecurity 125.00.01 Security of information and communication systems	***Objects of professional activity of graduates:*** - objects of Informatization, including computer, automated, telecommunication, information, information-analytical, information-telecommunication systems, information resources and technologies; - information security technologies; - management processes of information and / or cybersecurity of objects to be protected. ***Training objectives:*** *t*raining of specialists capable of using and implementing information and/or cybersecurity technologies ***Theoretical content of the subject activity. Knowledge:*** - legislative, regulatory and legal framework of Ukraine and the requirements of relevant international standards and practices for the implementation of professional activities; - principles of maintenance of information and/or cybersecurity systems and complexes; - theories, models and principles of access control to information resources; - theories of information and / or cybersecurity management systems; - methods and means of identification, management and identification of risks; - methods and means of evaluation and ensuring the necessary level of information security; - methods and means of technical and cryptographic protection of information - modern information and communication technologies; - modern software and hardware of information and communication technologies; - automated projecting systems ***Methods, techniques and technologies:*** methods, techniques and technologies of information and/or cybersecurity ***Tools and equipment:*** systems for development, maintenance, monitoring and control of information and/ or cybersecurity; modern software and hardware of information and communication technologies ***The proportion of the volumes of the general and professional components and optional parts:*** <u>Mandatory part (180 credits, 75 %):</u> - cycle of disciplines of humanitarian and socio-economic training (32 ECTS credits, 960 hours.); - cycle of disciplines of fundamental and natural science training (28 ECTS credits, 840 hours.); - cycle of disciplines of professional and practical training in the specialty (73 credits ECTS, 2190 hours.) and professional specialization (30 ECTS credits, 900 hours.) with writing 2 term

	papers in 3 and 5 semesters and producing bachelor's work (6 ECTS credits, 180 hours.) Parts of industrial (4 semester), technological (6 semester) and pre-diploma practice (8 semester): 15 ECTS credits, 450 hours Selective part (60 credits, 25 %). Of these, a specialized block of academic disciplines - 60 ECTS credits, 1800 hours.)
Orientation of the programme of study	Educational and professional program with an applied focus in the direction of security of information and communication systems.
The main focus of the programme of study	General: research in the field of practice and science of information security, organization and provision of information and / or cybersecurity at the objects of information activity
Specific features of the programme	In order to prepare for work in the real environment of future professional activities and graduates receive an educational qualification of a bachelor in cybersecurity, the program provides for students: - system theoretical knowledge in the field of it technologies with in-depth study of information and communication systems security specialization; - modern competences and practical skills of programming, development and management of databases, formation of models of protection and security policies, technical and cryptographic protection of information, construction of protected IP and TCP networks and maintenance of public key certificates, construction of complex information security systems (here and after – CCISS) at the objects of information activity and protection of automated systems from unauthorized access, testing of information and communication systems protection systems (here and after – ICS) for penetration, implementation of information and cybernetic security management, administration of protected ICS, monitoring and auditing, etc. In order to transfer the best practices to the future specialist, coverage in the educational process of the latest achievements of science and technology, the rules of successful business program provides: - implementation of the process approach in the construction of the context of profile-oriented academic disciplines, student's mobility, academic cooperation and youth exchanges; - involvement in teaching activities of managers and professionals who work in the system of vocational education and in the production of information technology and telecommunications, as well as business representatives.
4 - Eligibility of graduates to employment and further studying	
Suitability to employment opportunity	Graduates can work in the public and private sectors of Kyiv, Ukraine and the European Union in such areas: 1) administration of Windows/Linux, network equipment and technologies TCP/IP, DNS, DHCP, SSL / TLS, etc.; 2) application of anti-virus protection (ESET, McAfee, Zilly , etc.),

	software, client-server and cloud technologies for information protection (web filtering systems, intrusion prevention systems, mail protection systems against viruses and spam, etc.); 3) creation of technical, project and operational documentation of ICS) and information security systems (here and after-ISS); 4) configuration, exploitation and analysis of system processes of network, client-server and cloud technologies; 5) monitoring of unauthorized activity in computer systems; 6) creation, introduction and operation of CCISS) and also ICS as a part of information telecommunication and computer systems; 7) formation of policies and processes in the field of IT security, access control to network resources of its and information security risks; 8) investigation of incidents and audit of information security processes; 9) support for scientific research, teaching and pedagogical activity etc. According to the National Classification of Professions ДК 003: 2010, specialists who have completed training according to the programme of study "Security of information and communication systems" can occupy such primary positions as: - programmer / software tester of ICS systems; - administrator of computer systems and networks; - administrator of information and cyber security; - information and communication systems security auditor; -developer of information security tools; - engineer of service of technical protection of information etc.
Further learning	The possibility of obtaining education at the second (master's) level in the specialty 125 "cybersecurity" or other related (related) specialties of the field of knowledge "Information technology", which is consistent with the bachelor's degree, as well as other interdisciplinary master's programs with the IT component.
5 – Teaching and assessment	
Teaching and learning	Based on the principles of student-centered and individual-personal approach; implemented through training based on research, strengthening of practical orientation and creative orientation in the form of a combination of lectures, practical training, self-study and research using elements of distance learning, the solution of applied problems, the implementation of projects, educational and industrial practices, term papers, bachelor's work.
Assessment	Cumulative score-rating system, which provides for the evaluation of students for all types of classroom and extracurricular educational activities in the form of input, current, midterm and/or semester control, as well as certification.
6 – Competence of the graduate	
Integral competence	The ability to solve complex specialized tasks and practical problems in the field of information security and / or cybersecurity, which is characterized by the complexity and incomplete certainty of conditions.

	GC-1	The ability to apply knowledge in practical situations.
	GC-2	Knowledge and understanding of the subject area and understanding of the profession.
	GC-3	The ability to communicate professionally in the state and foreign languages not only orally but also in writing.
	GC-4	The ability to identify, set and solve problems of professional orientation
	GC-5	The ability to search, process and analyze information.
	GC-6	The ability to manage projects and conduct business
Professional Competences of specialty	PC- 1	The ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the implementation of professional activities in the field of information and/or cybersecurity.
	PC-2	The ability to use information and communication technologies, modern methods and models of information and/or cybersecurity.
	PC-3	The ability to use software and hardware complexes of information security in information and telecommunication (automated) systems.
	PC-4	The ability to ensure business continuity in accordance with established information and/or cybersecurity policies.
	PC-5	The ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information policy and/or cybersecurity.
	PC-6	The ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyberattacks, failures of different classes and origin.
	PC-7	The ability to implement and ensure the functioning of complex information security systems (complexes of legal, organizational and technical means and methods, procedures, practices, etc.)
	PC-8	The ability to implement procedures for incident management, investigate them and to evaluate them
	PC-9	The ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system.
	PC-10	The ability to apply methods and means of cryptographic and technical protection of information on objects of information activity.
	PC -11	The ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.
	PC-12	The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy.

7 – Programme learning outcomes	
PLO 1	- to prepare proposals for regulations and documents in order to ensure the established information and / or cybersecurity policy; - to develop project documentation, software and hardware complexes of information, information and telecommunication (automated) systems protection; - to perform analysis of the implementation of the adopted information policy and/or cybersecurity;
PLO 2	- to carry out professional activities on the basis of knowledge of modern information and communication technologies; - to develop and analyze ITC projects basing on standardized technologies and data transfer protocols; - to apply in professional activity knowledge, skills and practices regarding the structures of modern computing systems, methods and means of information processing, architectures of operating systems; - to protect resources and processes in ITC based on security models (finite state machines, flow control, Bell-LaPadula, Biba, Clark-Wilson, and others), and established modes of safe operation of ITC; - perform software analysis to assess compliance with established information and/or cybersecurity requirements in the its;
PLO 3	- to provide processes of protection of information and telecommunication (automated) systems by installation and correct operation of software and hardware complexes of means of protection; - to provide the functioning of special software, data protection software from the damaging effects of destructive codes into the information, information and telecommunication (automated) systems; - to carry out development of operational documentation on CMP:
PLO 4	- to solve the tasks of support (including: review, testing, reporting) of access control system according to the principles, access criteria and established security policy in information and information and telecommunication (automated) systems; - to implement measures to prevent unauthorized access to information resources and processes in information and information and telecommunication (automated) systems; - to solve problems of access control to information resources and processes in information and information and telecommunication (automated) systems on the basis of access control models (mandatory, discretionary, role-playing); - to solve the problems of centralized and decentralized administration with access to information resources and processes in information and information and telecommunication (automated) systems which based on access control models (mandatory, discretionary, role-playing); - to ensure accountability of the access control system of information resources and processes in ITC.
PLO 5	- to choose the main methods and means of information security in accordance with the requirements of modern standards of information and cybersecurity, and information technology security criteria, applying a systematic approach and knowledge of the basics of the theory of information security; - to solve problems of management of procedures of identification, authentication, authorization of users and processes in information and

	information and telecommunication (automated) systems - to project and implement complex systems of information security in the AS organization (enterprise) in accordance with the requirements of normative documents of the system of technical protection of information; - to solve problems of data flow protection in information, information and telecommunication (automated) systems; - to determine the level of security of information resources in information and information and telecommunication (automated) systems; - to use tools to assess the possibility of implementation of potential threats to information processed in information and telecommunications (automated) systems;
PLO 6	- to solve the problems of business continuity management using software and information resources reservation procedures; - to solve the problem of correcting the goals, strategies, plans to ensure business continuity after the implementation of cyberattacks, failures and failures of different classes; - to create and implement business continuity process plans; - to perform analysis of settings of information systems and communication equipment elements;
PLO 7	- to solve the problems of support and implementation of complex systems of information security, and also combating unauthorized access to resources and processes in information and information and telecommunication (automated) systems; - to estimate the level of security of information processed in ITC using the tools to assess the presence of potential vulnerabilities; - to solve problems of management of complex system of information security in information and information and telecommunication (automated); - solve the problems of examination, testing CCISS;
PLO 8	- to solve the problems of prevention and detection, identification, analysis and response to incidents in information, information and telecommunication (automated) systems; - to investigate information and/or cybersecurity incidents based on national and international regulations, procedures and regulations in the field of information and / or cybersecurity; - to ensure compliance with the event and incident logging policy with the specified level of details;
PLO 9	- to ensure the continuity of business processes of the organization on the basis of information security management system, according to domestic and international requirements and standards; - to ensure the functioning of the information and/or cybersecurity management system of the organization on the basis of information risk management, implementation of procedures for their quantitative and qualitative assessment;
PLO 10	- to analyze and determine the possibility of application of technologies, methods and means of cryptographic protection of information; - to analyze and determine the possibility of application of technologies, methods and means of technical protection of information;

	- to identify dangerous signals of technical means; - to measure the parameters of dangerous and interference signals during the instrumental control of information security from leakage by technical channels; - to determine the effectiveness of information protection from leakage by technical channels in accordance with the requirements of regulatory documents of the technical information protection system; - to interpret the results of special measurements using technical means to control the characteristics of its in accordance with the requirements of normative documents of the system of technical protection of information; - to substantiate the possibility of creating technical channels of information leakage at the objects of information activity; - to implement measures and means of technical protection of information from leakage by technical channels;
PLO 11	- to ensure the processes of monitoring of access to the resources and processes of ITC; - to ensure the configuration and functioning of systems of monitoring of resources and processes in its;
PLO 12	- to implement and support intrusion detection systems and use protection systems to ensure the necessary level of information security in information, information and telecommunications and automated systems; -to analyze the effectiveness of systems to detect and counter unauthorized access to resources and processes in its - to analyze and implement anti-malware systems.
8 - Resource support for the implementation of the programme	
Personnel support	Staffing of the educational and professional program consists mainly of the teaching staff of the Chair of Information and Cybernetic Security. In accordance with their competence and experience, the teaching staff of the Chair of Information Technologies and Mathematical Disciplines of the Faculty of the University are involved in teaching individual disciplines. The practice-oriented nature of the programme of study provides for a broad participation of practitioners corresponding to the direction of the program, which enhances the synergetic relationship of theoretical and practical training. The head of the project group and the teaching staff, which ensures its implementation, meets the requirements defined by the License conditions for the implementation of educational activities of educational institutions.
Material and technical support	Specially equipped with hardware and software, visual and methodological materials competence development centers, namely: 1) The Center of Research of Technologies of Functioning and Protection of Information and Communication Systems and Networks including educational Laboratory of Computer Networks and Cybersecurity, educational Laboratory of Safety ofIinformation and Communication Systems and educational Laboratory of Anti-virus Protection»; 2) The center for the Study of Technologies of Protection of Information Resources including educational Laboratory of Information Assets Security (educational cyber polygon) and educational Laboratory of Technical and Cryptographic Protection of Information;

	3) The Center of Modelling and Programming 4) Laboratory of Embedded Systems and 3D Modelling etc.
Information and educational-methodological support	Library electronic resources, electronic scientific publications, e-learning courses with the possibility of distance learning and independent work, Microsoft cloud services.
9 - Academic mobility	
National Credit Mobility	The regulation on the procedure of realization of the right to academic mobility of participants of the educational process of the University was put into effect by the order of 30.09.2016.
International Credit Mobility	Signed agreements on student mobility with universities of European countries in the framework of the Erasmus + programme KA1. Among them: the University of Vilnius (Lithuania), University of Constantine the Philosopher in Nitra (Slovakia), University of Extremadura (Spain), University of Silesia in Katowice (Poland), Academy of Jan Dlugosz in Czestochowa (Poland), University of Ostrava (Czech Republic), University of Paris-Sorbonne (France), University of Lisbon (Portugal) and others.
Studying of foreign higher education learners	The license provides for the training of foreigners and stateless persons.

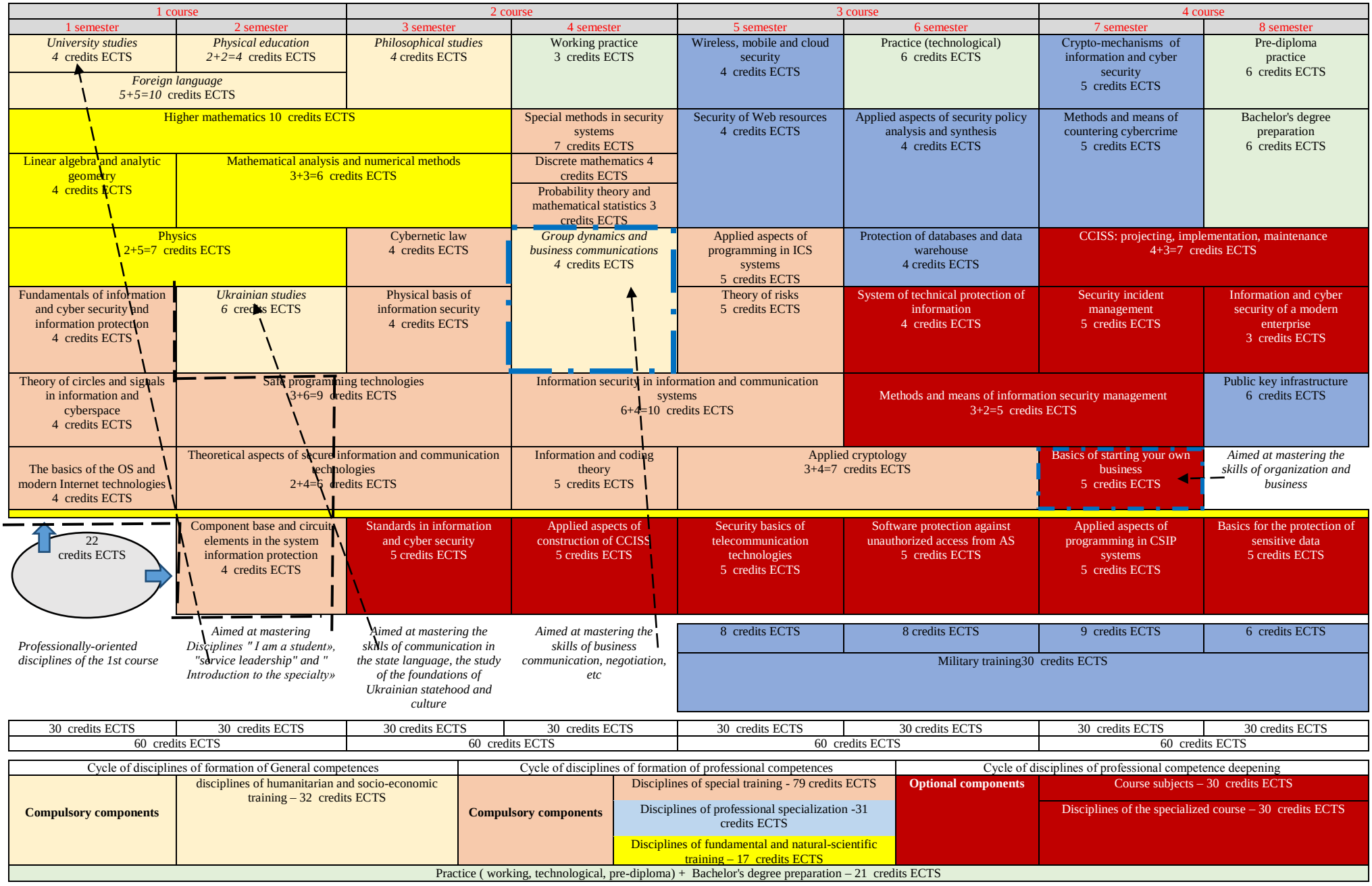
II. The List of the Components of the Programme of Study (vocational) Social Communications and Their Logical Coherence

2.1. The list and distribution of the volume of credit disciplines of the curriculum of training applicants for the first level of higher education-bachelor, specialty-125 Cybersecurity

Code	Components of the Programme of Study (academic discipline, practice, degree paper)	Credits	Distribution of class hours for courses and semesters								The Form of the Final Control
			1 course		2 course		3 course		4 course		
			1	2	3	4	5	6	7	8	
I. Compulsory components											
1. Educational discipline											
Formation of general competencies											
ОД3..01	*University studies*	**4**	4								Credit
	I'm a student	1	*								
	Leadership service	1	*								
	Introduction to the specialty	2	*								
ОД3..02	*Foreign language*	**10**	5	5							Exam, Credit
ОД3..03	*Physical education*	**4**	2	2							Credit
ОД3..04	*Ukrainian studies*	**6**		6							Exam
ОД3..05	*Philosophical studies*	**4**			4						Exam
ОД3..06	*Group dynamics and business communications*	**4**				4					Credit
	Amount	**32**	**11**	**13**	**4**	**4**	**0**	**0**	**0**	**0**	
The formation of a special (professional, subject-specific) competences											
ОДС.01	Physics	**7**	2	5							Exam, Credit
ОДС.02	Higher mathematics	**10**	4	3	3						Credit,Exam
	Linear algebra and analytic geometry	4	*								
	Mathematical analysis and numerical methods	6		*	*						
ОДС.03	Fundamentals of information and cyber security and information protection	**4**	4								Credit
ОДС.04	Theory of circles and signals in information and cyberspace	**5**	5								Exam
ОДС.05	The basics of the OS and modern Internet technologies	**4**	4								Credit
ОДС.06	Safe programming technologies	**9**		3	6						Exam. Credit, term paper
ОДС.07	Theoretical aspects of secure information and communication technologies	**6**		2	4						Exam, Credit
ОДС.08	Component base and circuit elements in the system.information protection	**4**		4							Exam
ОДС.09	Cybernetic law	**4**			4						Credit
ОДС.10	Physical basis of information security	**4**			4						Exam
ОДС.11	Special methods in security systems	**7**				7					Exam
	Discrete mathematics	4				*					
	Probability theory and mathematical statistics	3				*					
ОДС.12	Information security in information and communication systems	**10**				6	4				Exam, Credit term paper
ОДС.13	Information and coding theory	**5**				5					Exam
ОДС.14	Decision making in the information and cyber security	**5**					5				Exam
ОДС.15	Theory of risks	**5**					5				Credit
ОДС.16	Applied cryptology	**7**					3	4			Exam, Credit
ОДС.17	Wireless, mobile and cloud security	**4**					4				Exam
ОДС.18	Security of Web resources	**4**					4				Exam
ОДС.19	Applied aspects of security policy analysis and synthesis	**4**						4			Exam
ОДС.20	Protection of databases and data warehouse	**4**						4			Exam
ОДС.21	Crypto-mechanisms of information and cyber security	**5**							5		Exam
ОДС.22	Methods and means of countering cybercrime	**4**							4		Exam

ОДС.23	Public key infrastructure	**6**								6	Exam
	Amount	**127**	**19**	**17**	**21**	**18**	**25**	**12**	**9**	**6**	
2. Practice											
WP.2.01	Practice (working)	**3**				3					Credit
WP.2.02	Practice (technological)	**6**						6			Credit
WP.2.03	Pre-diploma	**6**								6	Credit
	Amount	**15**	**0**	**0**	**0**	**3**	**0**	**6**	**0**	**6**	
3. Certification											
C.01	Bachelor's degree preparation	**4,5**								4,5	
	Bachelor's thesis defense	**1,5**								1,5	
Amount		**6**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**6**	
	Total amount of the optional components	**180**	**30**	**30**	**25**	**25**	**25**	**18**	**9**	**18**	
II. Optional components											
4. Educational discipline											
4.1. Specialized block of academic disciplines											
OC.1.01	Standards in information and cyber security	**5**			5						Credit
OC.1.02	Applied aspects of construction of CCISS	**5**				5					Exam
OC.1.03	Security basics of telecommunication technologies	**5**					5				Exam
OC.1.04	Software protection against unauthorized access from AS	**5**						5			Exam
OC.1.05	Applied aspects of programming in CSIP systems	**5**							5		Exam
OC.1.06	Basics for the protection of sensitive data	**5**								5	Exam
OC.1.07	System of technical protection of information	**4**						4			Credit
OC.1.08	Methods and means of information security management	**5**						3	2		Credit
OC.1.09	CCISS: projecting, implementation, maintenance	**7**							4	3	Exam , term paper
OC.1.10	Security incident management	**5**							5		Credit
OC.1.11	Basics of starting your own business	**5**							5		Credit
OC.1.12	Information and cyber security of a modern enterprise	**4**								4	Credit
	Amount	**60**	**0**	**0**	**5**	**5**	**5**	**12**	**21**	**12**	
	4.2 Free choice academic disciplines from the course catalogue										
FC 1.01	Choice from the catalogue	**60**			5	5	5	12	21	12	Exam, Credit, term paper
	Total amount of the optional components	**60**	**0**	**0**	**5**	**5**	**5**	**12**	**21**	**12**	
TOTAL AMOUNT OF THE PROGRAMME OF STUDY		**240**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	

2.2. Structural Logical Scheme of the Programme of Study (Vocational)



3. Form of certification of applicants for higher education

Certification of applicants for higher education in the educational and professional program 125.00.01 Security of information and communication systems specialty 125 "Cybersecurity" is conducted by the examination Committee in accordance with the the Programme of Study (Vocational). The composition of the examination Committee may include representatives of employers and their associations, in accordance with the regulations on the examination Committee, approved by the academic Council of the University.
To certification allowed students who have fulfilled all the requirements of the training program (curriculum). Certification evaluates the totality of knowledge, skills, and other competencies acquired in the learning process. The term of certification is determined by the curriculum and schedule of the educational process.
Certification is carried out openly in the form of public protection of bachelor's work.
Certification ends with the issuance of a document of the established sample of the award person, successfully completed the educational and professional program of the bachelor's degree with the assignment of her qualification: Bachelor of Cybersecurity."

IV. Matrix of the Programme Competence Compliance with the Programme Components

Abbr. programme competences and programme components	ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ФК-1	ФК-2	ФК-3	ФК-4	ФК-5	ФК-6	ФК-7	ФК-8	ФК-9	ФК-10	ФК-11	ФК-12
CC.01	+	+																
CC.02			+															
CC.03					+													
CC 04			+															
CC.05	+																	
CC.06					+													
SP.01				+														
SP.02				+														
SP.03		+				+												
SP.04											+							
SP.05								+										
SP.06									+									
SP.07								+										
SP.08												+	+					
SP.09							+							+				
SP.10											+							
SP.11					+		+											
SP.12									+		+		+					
SP.13											+							
SP.14												+	+	+				
SP.15															+			
SP.16																+		
SP.17																	+	
SP.18																	+	
SP.19								+		+								
SP.20										+								
SP.21																+		
SP.22							+											
SP.23																		+
P.2.01	+	+	+	+	+	+	+	+										
P.2.02	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
P.2.03	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
C.01						+	+	+	+	+	+	+	+	+	+	+	+	+
OC.1.01							+											
OC.1.02													+					
OC.1.03											+							
OC.1.04										+								
OC.1.05									+									
OC.1.06																	+	+
OC.1.07													+			+		
OC.1.08															+			
OC.1.09													+					
OC.1.10														+				
OC.1.11						+				+								

Abbr. programme competences and programme components	ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ФК-1	ФК-2	ФК-3	ФК-4	ФК-5	ФК-6	ФК-7	ФК-8	ФК-9	ФК-10	ФК-11	ФК-12
ОС.1.12						+												+

V. Matrix of Providing Programme Learning Outcomes with the Relevant Programme Components

Abbr. programme competences and programme components	ПРН-1	ПРН-2	ПРН-3	ПРН-4	ПРН-5	ПРН-6	ПРН-7	ПРН-8	ПРН-9	ПРН-10	ПРН-11	ПРН-12
CC.01	+	+	+	+	+	+	+	+	+	+	+	+
CC.02	+	+	+	+	+	+	+	+	+	+	+	+
CC.03	+	+	+	+	+	+	+	+	+	+	+	+
CC.04	+	+	+	+	+	+	+	+	+	+	+	+
CC.05	+								+			
CC.06	+	+	+	+	+	+	+	+	+	+	+	+
SP.01		+				+			+			
SP.02		+	+									
SP.03		+	+									
SP.04		+	+									
SP.05		+	+									
SP.06			+	+	+	+	+	+	+	+	+	+
SP.07		+	+								+	
SP.08						+					+	
SP.09	+					+						
SP.10		+									+	
SP.11		+	+	+						+		
SP.12		+	+				+				+	+
SP.13				+						+		
SP.14					+	+			+			
SP.15									+			+
SP.16										+		
SP.17				+		+						
SP.18				+		+						
SP.19	+			+								
SP.20				+	+							
SP.21										+		
SP.22										+		
SP.23										+		
P.2.01	+	+	+	+	+	+	+	+	+	+	+	+
P.2.02	+	+	+	+	+	+	+	+	+	+	+	+
P.2.03	+	+	+	+	+	+	+	+	+	+	+	+
C.01	+	+	+	+	+	+	+	+	+	+	+	+
OC.1.01	+				+							
OC.1.02					+		+					
OC.1.03		+	+	+					+			
OC.1.04			+				+				+	+
OC.1.05			+	+	+	+	+	+	+	+	+	+
OC.1.06								+	+			+
OC.1.07			+				+					

Abbr. programme competences and programme components	ПРН-1	ПРН-2	ПРН-3	ПРН-4	ПРН-5	ПРН-6	ПРН-7	ПРН-8	ПРН-9	ПРН-10	ПРН-11	ПРН-12
ОС.1.08				+					+			
ОС.1.09					+		+					
ОС.1.10				+				+				
ОС.1.11						+			+			
ОС.1.12						+				+	+	+

*CC – Compulsory components
*SP – Special competences
P* - Practice
C*- Certification
OC*- Optional components
FC*- Free choice