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 Information and Communication System Security for Level Two (Master) of higher education

Field of Knowledge:	**12 Information Technologies**
Specialty	**125 Cyber Security**
Qualification**:**	**Master of Cyber Security**
Professional qualification**:**	**not regulated**

Enacted since 01 September 2018
(Order No.762, 28.11.2017)

Kyiv – 2017

LETTER OF APPROVAL

Programme of Study (Vocational)

The Chair of Information and Cyber Security

Faculty of Information Technology and Management

Borys Grinchenko Kyiv University

Protocol No.___, __ _______ 2018

The Head of the Chair ______________________ Volodymyr Buryachok

The Academic Council of the Faculty of Information Technology and Management of 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 Cyber Security for Level Two (Master) of higher education by the project group:

The Head of the project group:

Prof. Volodymyr Buryachok, PhD in Technical Sciences, the Head of the Chair of Information and Cyber Security of the Faculty of Information Technologies and Management of Borys Grinchenko Kyiv University

Members of the project group:

Prof. Anatoliy Bessalov, PhD in Technical Sciences, Professor of the Chair of Information and Cyber Security of the Faculty of Information Technologies and Management of Borys Grinchenko Kyiv University

Prof. Serhiy Toliupa, PhD in Technical Sciences, Professor of the Chair of Information and Cyber Security of the Faculty of Information Technologies and Management of Borys Grinchenko Kyiv University (part-time)

Vadym Abramov,Candidate of Technical Sciences, Associate Professor, Associate Professor of the Chair of Information and Cyber Security of the Faculty of Information Technologies and Management of Borys Grinchenko Kyiv University

Reviewers:

1. *Prof. Oleksii Smirnov, PhD in Technical Sciences, the Head of the Chair of Cyber Security and Software of Central Ukrainian National Technical University, Kropyvnytskyi*
2. *Viacheslav Tatianin, Candidate of Technical Sciences, Senior Research Fellow, the Director of "AVTOR"Ltd, Kyiv*

The programme of study (vocational) is introduced for the first time.

The term for the review of the programme of study: ___ times in ___ years

Actualized:

Date of Review of the PS /Amendments to PS			
Signature:_________			
Full name of the PS guarantor			

1. PROFILE OF THE PROGRAMME OF STUDY (VOCATIONAL)

125 CYBER SECURITY

1 - General information

The full name of the higher education institution and the structural unit	Borys Grinchenko Kyiv University Faculty of Information Technology and Management
Degree of higher education	Master Master of Cyber Security Professional qualification is not regulated
Official name of the programme of study	125.00.02 Information and communication system security
Type of diploma and term of study according to the programme	Master degree, unitary, 90 credits ECTS term of study: 1 year 4 months
Availability of accreditation	Implementation/Accreditation in 2018
Cycle / Level	Level Two (Master) / FQ-EHEA – second cycle, QF LLL – Level Seven, HPK – Level Eight
The education level required to commence study under the programme	Level One (Bachelor) of higher education
Language (s) of teaching	Ukrainian
Validity of the programme of study	2021
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 fundamental training in the form of profound theoretical and practical knowledge, skills and abilities within the specialty 125 Cyber Security, sufficient for effective performance of tasks of an innovative nature on the corresponding level of professional activity in the field of information and telecommunication technologies, pedagogy and methodology of higher education.

3 - Characteristics of the programme of study

Subject area: **12 Information Technologies** **125 Cyber Security** **125.00.01 Information and**	*Objects of professional activity of graduates:* -objects of informatization, including computer, computer-based, data-processing, information and telecommunication systems, information resources and technologies; - information security technologies; - processes for managing the information and/or cyber security of objects to be protected. *Learning objectives:* training of professionals capable of using and implementing technologies as well as using information and/or cyber security

Communication System Security	methods *The theoretical content of the subject area includes thorough knowledge of*: - the legislative and regulatory frameworks of Ukraine and the requirements of the relevant international standards and practices for the pursuit of professional activities; - principles of maintenance of information and/or cyber security systems and complexes; - theories, models and principles of access control to IP; - information and / or cyber security management systems theories; - methods and means for detecting, managing and identifying 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; - computer-based design systems. *Methods, techniques and technologies:* methods, techniques and technologies for providing information and/or cyber security. *Instruments and equipment:* systems of the development, provision, monitoring and control of information and/or cyber security; modern hardware and software of information and communication technologies. *The proportion of the volumes of the general and professional components and optional parts:* General and special (professional) competencies for the speciality (63 ECTS credits, 70%): - a cycle of disciplines of professionally oriented humanitarian, socio-economic and natural science training (13 ECTS credits, 390 hours); - a cycle of special training courses (20 ECTS credits, 600 hours) and specialization (12 ECTS credits, 360 hours) with 1 term paper in the 9th semester and master's thesis (6 ECTS credits, 180 hours). The share of research (Semester 11), work-experienced (technological) (Semester 11) and pre-diploma practices (Semester 11): 12 ECTS credits, 13%, 360 hours. Optional part (27 ECTS credits, 30%), among which a specialized block of academic disciplines contains: - the discipline of course preparation (8 ECTS credits, 240 hours); - the discipline of a specialized course (19 ECTS credits, 510 hours).
Orientation of the programme of study	The programme of study with an applied focus on the specialization “Information and communication system security”
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 cyber security of objects to be protected.
Specific features of the	In order to prepare the graduates for work in the real environment of the future professional activities and obtain the educational qualification of the Master of

programme	Cyber Security, the program provides training of professionals capable of: - detecting and evaluating the signs of extraneous cybernetic effects; - modeling possible situations of third-party cybernetic influence and predicting their possible consequences; - organizing and maintaining a set of measures to ensure information and/or cyber security; - conducting research in the areas of information and/or cyber security protection of national interests of Ukraine and substantiate ways to increase its effectiveness; - counteracting the unauthorized penetration of the opposing sides to their own IT systems and networks, ensuring the stability of their work, as well as restoring their normal functioning after the implementation of cyber-attacks; - providing cryptoprotection of their own information resource, etc. In order to share the best practices with the future professional, coverage of the latest achievements in science and technology in the educational process and the rules for conducting successful business, the program provides: - implementation of the process approach in constructing the content of profile-oriented academic disciplines, student mobility, academic cooperation and youth exchanges; - engagement in teaching activities of directors and professionals working either in the system of vocational education, or in the field of information technologies and telecommunications, as well as business representatives.
4 - Eligibility of graduates to employment and further studying	
Eligibility to employment	Graduates can work in the public and private sectors of Kyiv, Ukraine and the European Union in the following areas: 1) administering Windows / Linux OS, network equipment and TCP/IP, DNS, DHCP, SSL/TLS technologies, etc .; 2) the usage of antivirus protection tools (ESET, McAfee, Zilly, etc.), software, client-server and cloud-based information security technologies (web filtering systems, attack preventing systems, mail security systems against viruses and spam, etc.); 3) creation of technical, project and operational documentation of information and communication systems (thereafter - ICS) and information security systems (hereafter - ISS); 4) customization/setup, exploitation and analysis of system processes of network, client-server and cloud-based technologies; 5) monitoring of unauthorized activity in computer systems; 6) developing, implementing and operating the integrated information security systems (thereafter "IISS"), as well as ISS within the information telecommunication (thereafter - ITS) and computer systems; 7) policy-making/processes and policy formulation in the field of IT security, managing the access to ITS network resources and information security risks; 8) conducting incident investigations and ensuring the audit of information security processes; 9) support for scientific research, pedagogical activities, etc. According to the National Classification of Professions DK 003: 2010, specialists who have obtained the diploma in the PS "Information and Communication System Security " may hold following initial positions: - programmer/examiner of information and cyber security systems software;

	- administrator of computer systems and networks; - administrator of information and cyber security; - auditor/pentester of ICS security; - developer of information protection tools; - a leading specialist/head of the technical information security service, etc.
Further learning	Possibility to study at the Level Three of higher education in specialty 125 "Cyber Security" or other related (adjacent) specializations in the field of "Information Technologies" that are consistent with the obtained Master degree, other interdisciplinary Master programs with the IT component. Possibility of advanced training and obtaining additional postgraduate education.

5 – Teaching and assessment

Teaching and learning	Based on the principles of student-centered and individually personal approach; teaching and learning are realized through studies based on research, strengthening of practical and creative orientation in the form of lectures, practical classes, independent academic and research work combination using the elements of distance learning, solving applied problems, project conduction, training and field practices, term and degree papers.
Assessment	Accumulation rating system, which involves assessing students for all types of face-to-face and extracurricular educational activities in the form of entrance, routine, degree and/or semester control and certification.

6 - Programme competencies

Integral competence	Ability to solve complex specialized tasks and practical problems in the field of information and/or cyber security, characterized by complexity and incomplete certainty of conditions.	
General competence (GC)	GC-1	Ability to communicate professionally in a foreign language
	GC-2	Ability to acquire new knowledge, accumulate and apply scientific and pedagogical abilities in practical situations.
	GC-3	Ability to identify, generate, analyze and solve problems in the professional field.
Professional competence (PC)	PC-1	Ability to apply modern information and security technologies in the field of information security
	PC-2	Ability to detect vulnerabilities and provide wired and wireless network security, investigate information and/or cyber security incidents and counteract malware.
	PC-3	Ability to ensure the safety of Web resources, restore its regular functioning as a result of crashes and failures of different forms and origins.
	PC-4	Ability to secure information network resources and cryptographic protection in information and/or cyber security systems.
	PC-5	Ability to ensure the protection of information processed in information and communication systems, as well as administrate and operate them.

7 - Programme learning outcomes

Knowledge and understanding	PLO1	- ability to apply knowledge of foreign languages to provide the effectiveness of professional communication;

		- ability to diagnose and interpret situations, plan and conduct scientific research, critically comprehend the fundamental theories, principles, methods and concepts in studying and professional activity; - ability to represent obtained knowledge and skills of the theory and practice of ISS in oral and/or written form in front of a professional and non-professional audience;
	PLO 2	- ability to identify and formulate actual scientific problems, generate and integrate new ideas and knowledge in the field of information and/or cyber security; - ability to apply specialized software packages, modern information and/or security technologies in the field of information security; - to know the vulnerability and methods of its application in various telecommunication technologies; - to know how to deal with the vulnerability, as well as to be aware of specialized network equipment used to secure corporate networks; - ability to design protected wired telecommunication systems (taking into account possible threats); - to know the methods of organizing secure data transmission in an unprotected environment;
	PLO 3	- to know the vulnerability and methods of its application in in wireless and mobile networks; - ability to detect threats of penetration or attacker’s access to such networks; - to know the specialized network equipment used to provide the safety of wireless and mobile networks; - to be able to design protected wireless networks (taking into account possible threats);
	PLO 4	- to know the methods of developing and testing software for detecting and eliminating activities that threaten system security (antivirus, firewalls, sniffers, port scanners);
	PLO 5	- ability to conduct semantic analysis of files; - ability to detect malware according to its structure and mode of behavior; - ability to recover damaged information; - ability to model software vulnerability and use design patterns to protect software;
	PLO 6	- to know the existing vulnerability of Web resources (SQL injections, brute-force, XSS, etc) and ways to deal with them during the development phase and in the following process of deployment; - know the design patterns of secure Web applications;
	PLO 7	- to know the methods of network resources testing for security vulnerability; - ability to eliminate it;
	PLO 8	- ability to organize the processes of incidents investigation in accordance with the standards of ISO 27001, ISO 20000, ISO / IEC TR 18044, NIST SP 800-61, CMU / SEI-2004-TR-015, ISO 27035, ISO 27037. ISO 27031;

	PLO 9	- to have practical skills in conducting security audits of ICS, its administration and exploitation; - ability to design perspective cryptosystems and apply modern technologies of cryptographic protection of information in information and/or cyber security systems.

8 - Resource support for the implementation of the programme

Personnel support	The personnel support of the programme of study consists of the academic staff of the Chair of Information and Cyber Security. The academic staff of the Chair of Information Technologies and Mathematical Sciences of the faculty of Information Technology and Management (FITM) is involved in the teaching of certain disciplines in accordance with their competence and experience. The practice-oriented PS involves the broad participation of practical experts who correspond to the specialization of the programme, which enhances the synergy of theoretical and practical training. The head of the project team and the academic staff, that ensure its implementation, comply with the requirements specified by the License terms for conducting academic activity of educational institutions.
Material and technical support	Competence development centers are well-equipped with hardware and software, visual and methodological materials: 1) "Research Center of Operation Technologies and ICS and Network Security " with: – "Computer Network and Cyber Security Laboratory", – "ICSS Laboratory " – "Antivirus Protection Laboratory"; 2) "Research Center of Information Resources Security Technologies" with: – "Information Asset Security Laboratory" (educational cyberpolygon) – "Technical and Cryptographic Information Security Systems Laboratory "; 3) "Modeling and Programming Center" 4) "Laboratory of embedded systems and 3D modeling", etc.
Information and educational-methodological support	Librarian electronic resources, electronic scientific editions, electronic training courses with the possibility of distance learning and independent work, Microsoft cloud services.

9 - Academic mobility

National Credit Mobility	The Regulation on the procedure for the implementation of the right on academic mobility of participants in the educational process of the University was put into effect by order of 30.09.2016
International Credit Mobility	Agreements on student mobility with the Pomorskaya Academy in Slupsk (Poland), Vilnius University (Lithuania) Erasmus + CA1 Program with Foggia University (Italy), University of Cadiz (Spain) Agreements on student mobility with universities in European countries and within the Erasmus + KA1programme: University of Vilnius (Lithuania), Constantine the Philosopher University in Nitra (Slovakia), University of Extremadura (Spain), University of Silesia in Katowice (Poland), Jan

	Długosz Academy in Częstochowa (Poland),University of Ostrava (Czech Republic), Paris-Sorbonne University (France), University of Lisbon (Portugal) and others.
Studying of foreign higher education learners	According to the License, the preparation of foreigners and stateless persons is envisaged.

2. The List of the Components and their Logical Coherence of the Programme of Study (vocational)

2.1. List and distribution of credit volume of disciplines for the preparation in the field of study 125 "Cyber Security" for Level Two (Master degree) of higher education (90 credits ECTS - 1 year 4 months)

Component Code	Components of the Programme of Study (academic discipline, practice, degree paper)	Credits ECTS	Distribution of hours by academic years and semesters			The Form of the Final Control
			Year of Study 5		Year of Study 6	
			semester			
			9	10	11	
1.	**Compulsory components of PS**					
1. Academic disciplines						
Formation of special (professional, objective) competencies						
ОДФ.01	Foreign language/for professional purpose	**5**	3	2		Credit
ОДФ.02	Research and science organization	**4**	4			Credit
ОДФ.03	General applied theory of security systems	**4**	4			Exam
ОДФ.04	Network infrastructure security technologies	**7**	7			Exam, TP
ОДФ.05	Wireless and mobile network security technologies	**7**	7			Credit
ОДФ.06	Web-resources security technologies	**6**		6		Exam
ОДФ.07	Security Investigation Technologies	**6**		6		Credit
ОДФ.08	Applied aspects of penetration and ethical hacking testing	**6**		4	2	Credit, Exam
	Total	**45**	**25**	**18**	**2**	
2. Practice						
ОП.01	Field (Technological) Practice	**3**			3	Credit
ОП.02	Scientific research practice	**3**			3	Credit
ОП.03	Pre-diploma practice	**6**			6	Credit
	Total	**12**	**0**	**0**	**12**	
3. Certification						
ОА.1	Preparation of Qualification Master Degree Paper	**4,5**		4,5		
	Master Degree Paper Defense	**1,5**			1,5	
	Total	**6**	**0**	**4,5**	**1,5**	
Total amount of the compulsory components		**63**	**25**	**22,5**	**15,5**	
2	**Optional components of PS**					
4. Academic disciplines						
4.1.Specialized block of Academic disciplines						
ВДС.01	Monitoring and administration of secure IT systems and networks	**7**	5	2		Credit, Exam
ВДС.02	Technologies of development and network security software testing	**6**		6		Exam
ВДС.03	Malware counteraction technologies	**6**			6	Exam
ВДС.04	Mathematical methods of cryptography	**4**		4		Credit
ВДС.05	Methods of construction and cryptosystem analysis	**4**			4	Credit
Total amount of the optional components		**27**	**5**	**12**	**10**	
4.2. Free choice of academic disciplines from the course catalogue (a student chooses academic disciplines in accordance with following ECTS credits)						
ВД 1.01	The choice from the course catalogue	**27**	5	12	**10**	Credit, Exam
Total amount of the optional components		**27**				
TOTAL AMOUNT OF THE PROGRAMME OF STUDY		**90**	**30**	**34,5**	**25,5**	

2.2 Structurally logical framework of PS

Year of Study 5				Year of Study 6	
Semester 9		Semester 10		Semester 11	
Foreign language of professional direction, 3+2= 5 credits				Methods of construction and cryptosystem analysis, 4 credits	Scientific research practice, 3 credits
Research and science organization, 4 credits	Network infrastructure security technologies, 7 credits	Web-resources security technologies, 6 credits	Mathematical methods of cryptography, 4 credits		Field (Technological) Practice, 3 credits
General applied theory of security systems, 4 credits	Wireless and mobile network security technologies, 7 credits	Security Investigation Technologies, 6 credits	Technologies of development and network security software testing, 6 credits	Malware counteraction technologies, 6 credits	Pre-diploma practice, 6 credits
Monitoring and administration of secure IT systems and networks, 5+2=7 credits			Applied aspects of penetration and ethical hacking testing, 4+2=6 credits		Preparation of Qualification Master Degree Paper, 6 credits

3. Form of Certification for higher education applicants

Certification of higher education learners taking PS 125.00.02 "Information and communication system security", specialty 125 "Cyber security" is conducted by the examination commission in accordance with the requirements of the programme. The examination commission may include representatives of employers and their associations, in accordance with the regulations on the examination commission approved by the Academic Council of the University.

Students who have fulfilled all the requirements of the PS are admitted to the certification. The certification includes a set of knowledge, skills, other competences acquired by students in the studying process. The certification date is determined by the curriculum and the timetable of the studying process.

The certification is conducted openly in the form of public defense of the qualification master degree paper. Having passed the certification, the student who has successfully completed the PS is issued with the document of the standard form leading to the corresponding master degree qualification: "Master of Cyber Security".

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

	GC-1	GC-2	GC-3	GC-1	GC-2	GC-3	GC-4	GC-5
ОДФ.01	+							
ОДФ.02		+						
ОДФ.03			+					+
ОДФ.04				+				+
ОДФ.05					+			+
ОДФ.06						+		
ОДФ.07					+			+
ОДФ.08							+	+
ВДС.01								+
ВДС.02					+			
ВДС.03					+			
ВДС.04							+	
ВДС.05							+	
ОП.01	+	+	+	+				
ОП.02			+	+	+	+		
ОП.03	+	+	+	+	+	+	+	+
ОА.1	+	+	+	+	+	+	+	+

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

	PLO -1	PLO -2	PLO -3	PLO -4	PLO -5	PLO -6	PLO -7	PLO -8	PLO -9
ОДФ.01	+								
ОДФ.02	+	+							
ОДФ.03	+								
ОДФ.04		+	+				+		+
ОДФ.05			+						+
ОДФ.06						+			
ОДФ.07								+	+
ОДФ.08				+	+				+
ВДС.01									+
ВДС.02		+		+					
ВДС.03		+		+	+				
ВДС.04									+
ВДС.05									+
ОП.01	+	+	+	+	+	+	+	+	+
ОП.02	+	+	+	+	+	+	+	+	+
ОП.03	+	+	+	+	+	+	+	+	+
ОА.1	+	+	+	+	+	+	+	+	+

The Head of the Project Group (PS Guarantor)

Professor of the Chair of Information Technologies and Mathematical Sciences of the Faculty of Information Technologies and Management of Borys Grinchenko Kyiv University, PhD in Technical Sciences

Prof. Volodymyr Buryachok