BORYS GRINCHENKO KYIV UNIVERSITY

«APPROVED»
Decision of the Academic Board of
Borys Grinchenko Kyiv University,
June 17, 2021, Protocol No. 6

Chief of the Academic Board, Rector
_____ Viktor OGNEVIUK

EDUCATIONAL AND PROFESSIONAL PROGRAM

125.00.01 Security of information and communication systems

of the second (master's) level of higher education

Field of Knowledge:	12 Information Technology
Specialty:	125 Cyber Security
Qualification:	Master in Cyber Security

(new edition)

Enacted since September 1, 2021
(Order No. ____, dated ____, ____)

Kyiv – 2021

LETTER OF APPROVAL
New edition of the educational and professional program
"Security of information and communication systems"
second (master's) level of higher education

The Program was revised and updated in 2021.

Chair of Information and Cyber Security
Protocol No. 6 from May 12, 2021
Head of the Chair _____

Academic Council of the Faculty of Information Technology and Management
Protocol No. __ from June 6, 2021
Head of the Academic Council _____ Alla MYKHATSKA

Scientific and Methodological Centre of Standardization and Quality of Education

Head _____ Olha LEONTIEVA

_____ ___, 2021

Vice-Rector on Academic Affairs

_____ Oleksii ZHYLTSOV

_____ ___, 2021

PREFACE

Educational and professional program "Security of Information and Communication Systems" is developed on the basis of the Law of Ukraine "On Higher Education" and the Standard of Higher Education of Ukraine in the field of knowledge 12 Information Technology specialty 125 "Cybersecurity" for the second (master's) level of higher education from March 18, 2021 № 332.

IT IS DRAFTED by the project group consisiting of:

Sokolov V.Y. – Candidate of Technical Sciences, Associate Professor of the Chair of Information and Cyber Security (guarantor of the educational program).

Semko V.V. – Doctor of Technical Sciences, Associate Professor, Professor of the Chair of Information and Cyber Security.

Bessalov A.V. – Doctor of Technical Sciences, Professor, Professor of the Chair of Information and Cyber Security.

Tsyrkaniuk D.A. – student of the educational and professional program "Security of Information and Communication Systems" 2020 - 2021 years of the Faculty of Information Technology and Management of Borys Grinchenko Kyiv University.

EXTERNAL REVIEWERS:

Trofimchuk Oleksandr Mykolayovych – Corresponding Member of the National Academy of Sciences of Ukraine, Doctor of Technical Sciences, Professor, Director of the Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine

Lukova-Chuiko Nataliia Viktorivna – Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity and Information Protection of Taras Shevchenko National University of Kyiv

REVIEWS OF EMPLOYER'S REPRESENTATIVES:

Yermoshyn Valerii Vitaliiovych - Candidate of Technical Sciences, Director of the Information Security Department of NPC "Ukrenergo"

The educational program was put into effect on September 1, 2018.
Deadline for reviewing the educational program is once a year.

Updated:

Date of review	March 2021			
Signature				
Name of the EP guarantor	Sokolov V.Y.			

Substantiation

Updates of the educational and professional program "Security of Information and Communication Systems" were made due to the need to coordinate the content of the educational and professional program approved by the Academic Council of Borys Grinchenko Kyiv University from May 25, 2017, protocol № 5 (Order from May 26, 2017, № 348), as amended by August 29, 2019, protocol № 7 (Order from August 30, 2019, № 509) and the approved standard of higher education in the 125 "Cybersecurity" specialty for the second (master's) level of higher education, as well as several factors that emerged in the implementation of the educational program during 2019- 2020, 2020-2021 academic years and offers received from the stakeholders (graduates and employers).

During the work on the implementation of the curriculum, development of work programs of disciplines, filling of electronic training courses, as well as during internships and certification, the working group received feedback from teachers, practice bases and employers with a number of wishes to optimize certain components of the educational program. After consultations and workshops, the working group agreed on several changes to certain components of the 125.00.01 "Security of information and communication systems" EPP.

Clarifications to the description of the educational-professional program, taking into account the approved standard of higher education in the specialty 125 Cybersecurity for the second (master's) level of higher education (Order of the Ministry of Education and Science of Ukraine from June 20, 2019, № 871), were included in the following sections:

- general information;
- list of the graduate’s program competencies;
- learning outcomes.

The main changes in the curriculum were:

- structural and logical swquence;
- redistribution of the number of credits between the different educational components;
- re-planning of the time-limits for internships.

The new version of these parts of the educational and professional program is contained below.

I. Profile of the educational program
125.00.01 Security of information and communication systems

1 - General information	
Full name of the institution of higher education and the structural unit	Borys Grinchenko Kyiv University Faculty of Information Technologies and Management
Level of higher education	Second (master's) level
Degree of higher education	Master
Field of knowledge	12 Information technologies
Specialty	125 Cyber Security
Educational program	Educational and professional program "Security of information and communication systems"
Qualification	Master in Cyber Security
Qualification in diploma	degree of higher education - Master specialty – Cyber Security educational program - Security of information and communication systems
Form of study	Institutional (full-time)
Language (s) of instruction	Ukrainian language. Some educational components are taught in English.
Cycle / level	HPK - level 7, FQ-EHEA - the second cycle, EQF LLL - level 7;
Type of diploma and volume of the educational program	Master's degree, single, 90 ECTS credits, term of study – 1 year and 4 months
Prerequisites	Availability of a bachelor's degree
Availability of accreditation	National Agency for Quality Assurance in Higher Education. Ukraine. Certificate of exemplary accreditation of the educational program "Security of Information and Communication Systems" educational program in the specialty 125 Cybersecurity, in the level of a master's degree Certificate: № 113 dated January 16, 2020 Valid until – January 13, 2025
Internet address of the permanent placement of the description of the educational program	http://kubg.edu.ua/informatsiya/vstupnikam/napryami-pidgotovki/
2 - The purpose of the educational program	
Provide applicants with fundamental training in the form of in-depth theoretical and practical knowledge, skills and abilities in the specialty 125 Cybersecurity, sufficient for the effective implementation of innovative tasks of the appropriate level of professional activity in the fields of telecommunications and information technology.	

3 - Characteristics of the educational program	
Description of the subject area	**Objects of study:** – modern processes of research, analysis, creation and operation of information systems and technologies, other business operational processes at the objects of information activities and critical infrastructures in the field of information security and / or cybersecurity; – information systems (information and communication, information and telecommunication, automated) and technologies; – infrastructure of information objects and critical infrastructures; – systems and complexes of creation, processing, transmission, storage, destruction, protection and display of data (information flows); – information resources of different classes (including information resources of different categories); – software and hardware (means) of cybersecurity; – information security and / or cybersecurity management systems; – technologies, methods, models and means of information security and / or cybersecurity. **Learning objectives** Training of specialists capable of solving research and / or innovation tasks in the field of information and / or cybersecurity. **Theoretical content of the subject area** Theoretical principles of science-intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision making, systems analysis, complex systems, process modeling and optimization, theory of mathematical statistics, cryptographic and technical protection of information, risk theory and other interdisciplinary theories and practices in information security and / or cybersecurity. **Methods, techniques and technologies** Methods, models, techniques and technologies for creating, processing, transmitting, receiving, destroying, displaying, protecting (protecting) information resources in cyberspace, as well as methods and models for developing and using applied and specialized software to solve professional problems in information security and / or cybersecurity. Technologies, methods and models of research, analysis, management and support of business / operational processes using a set of legal and organizational-technical methods and means of protecting information resources in cyberspace. **Tools and equipment** Tools, devices, network equipment and environment, application and specialized software, automated systems and complexes of design, modeling, operation, control, monitoring, processing, display and protection of data (information flows), as well as methods and models of risk theory and information management resources for research and support of information activities in the field of information security and / or cybersecurity.

Program structure	The ratio of the volume of mandatory (general and professional) and elective components of the EP: Mandatory part (64 credits, 71%): disciplines aimed at the formation of general and special (professional) competencies (43 credits), practice (15 credits), certification (6 credits). Elective part (26 credits, 29%): disciplines of free choice
4 – Suitability of graduates for employment	
Suitability for employment	Graduates can work in the public and private sectors of Kyiv, Ukraine and the European Union in the following areas: administration of Windows / Linux, network equipment and technologies TCP / IP, DNS, DHCP, SSL / TLS, etc .; application of anti-virus protection (ESET, McAfee, Zilly, etc.), software, client-server and cloud information protection technologies (web filtering systems, intrusion prevention systems, mail protection systems against viruses and spam, etc.); creation of technical, design and operational documentation of information and communication systems (hereinafter - ICS) and information protection systems (hereinafter - IPS); debugging, operation and analysis of system processes of network, client-server and cloud technologies; monitoring of unauthorized activity in computer systems; creation, implementation and operation of integrated information security systems (hereinafter - IPS), as well as IPS as part of information and telecommunications (hereinafter - ITS) and computer systems; formation of policies and processes in the field of IT security, management of access to ITS network resources and information security risks; conducting investigations of incidents and ensuring the audit of information security processes; support of scientific research, pedagogical activity, etc. According to the National Classification of Occupations DK 003: 2010, specialists who have been educated in the educational program "Security of Information and Communication Systems" can hold such primary positions as: 2149.2 Information Security Professional
Further study	Education at the third (educational and scientific) level of higher education. Acquisition of additional qualifications in the system of postgraduate education.
5 – Teaching and assessment	
Teaching and assessment	The educational process is based on the principles of: student-centered, personality-oriented learning, competence, system-integrative approaches, research-based learning. Teaching is carried out in the form of: lectures, seminars, practical classes, laboratory work. Independent work is provided (performance of individual tasks, defense of course work;); consultations with teachers; e-learning for individual educational components, internships, writing a master's thesis. E-learning, group project work, mentoring of practitioners, training in practical training centers are being introduced. Encouraging higher education students and organizing group work in order to acquire teamwork skills and independently find a solution to the problem, in particular, when solving practical cases.

Evaluation	Accumulative point-rating system for the assessment of students for all types of classroom and extracurricular educational activities in the form of intermediate, final (semester) control, as well as certification. Intermediate control (oral examination, written express control / computer testing, etc.), modular control, final semester control (tests, exams in oral, written (testing), combined forms, defense of term papers, defense of practice reports), certification (defense of qualifying master's thesis). Assessment of higher education students is in accordance with the Unified system of assessment of academic achievement of students of Borys Grinchenko Kyiv University.
6 - Program competencies	
Integral competence	Ability to solve complex specialized problems and practical problems in the field of information and / or cybersecurity, characterized by complex and incomplete definition of conditions.
General competencies (GC)	**GC 1** Ability to apply knowledge in practical situations.
	GC 2 Ability to conduct research at the appropriate level.
	GC 3 Ability to abstract thinking, analysis and synthesis.
	GC 4 Ability to evaluate and ensure the quality of work performed.
	GC 5 Ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / economic activities).
	GC 6 Ability to communicate professionally in a foreign language
Special (professional, subject) competencies (SC)	**SC 1** Ability to reasonably apply, integrate, develop and improve modern information technologies, physical and mathematical models, as well as technologies for creating and using application and specialized software to solve professional problems in the field of information security and / or cybersecurity.
	SC 2 Ability to develop, implement and analyze regulations, regulations, instructions and requirements of technical and organizational direction, as well as to integrate, analyze and use world best practices, standards in professional activities in the field of information security and / or cybersecurity.
	SC 3 Ability to research, develop and maintain information security and / or cybersecurity methods and tools at information facilities and critical infrastructure.
	SC 4 Ability to analyze, develop and maintain the information security and / or cyber security management system of the organization, to form information security strategies and policies taking into account national and international standards and requirements.
	SC 5

	Ability to research, systemically analyze and ensure the continuity of business / operational processes to identify vulnerabilities in information systems and resources, analyze risks and assess their impact in accordance with the established strategy and policy of information security and / or cybersecurity of the organization.
	SC 6 Ability to analyze, control and provide access control system to information resources in accordance with the established strategy and policy of information security and / or cybersecurity of the organization.
	SC 7 Ability to research, develop and implement methods and measures to combat cyber incidents, to implement management, control and investigation procedures, as well as to provide recommendations for the prevention and analysis of cyber incidents in general.
	SC 8 Ability to research, develop, implement and maintain methods and means of cryptographic and technical protection of information at information facilities and critical infrastructure, information systems, as well as the ability to assess the effectiveness of their use, according to established strategy and policy of information security and / or cybersecurity of an organization.
	SC 9 Ability to analyze, develop and maintain a system of auditing and monitoring the effectiveness of information systems and technologies, business / operational processes in the field of information security and / or cybersecurity of the organization as a whole.
	SC 10 Ability to conduct research and teaching activities, plan training, monitor and support work with staff, as well as make effective decisions on information security and / or cybersecurity.
	SC 11 Ability to use modern security information and SMAR-technologies in the field of information security.
	SC 12 Ability to detect vulnerabilities and ensure the security of telecommunications technologies and SMART infrastructure. investigation of information and / or cybersecurity incidents and counteraction to malicious software
7 – The normative content of higher education training, formulated in terms of learning outcomes	
PLO 1 Fluent in state and foreign languages, orally and in writing to present and discuss research and innovation results, business / operational processes and professional information security and / or cybersecurity issues.	
PLO 2 Integrate fundamental and expertise to address complex information security and / or cybersecurity challenges in broad or multidisciplinary contexts.	
PLO 3	

Conduct research and / or innovation activities in the field of information security and / or cybersecurity, as well as in the field of technical and cryptographic protection of information in cyberspace.
PLO 4 Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and / or cybersecurity.
PLO 5 Critically comprehend the problems of information security and / or cybersecurity, including at the intersectoral and interdisciplinary level, in particular based on the understanding of new results in engineering and physical and mathematical sciences, as well as the development of technologies for creating and using specialized software.
PLO 6 Analyze and evaluate the security of cybersecurity systems, complexes and tools, technologies for creating and using specialized software.
PLO 7 Justify the use, implementation and analysis of the best world standards, practices in order to solve complex problems of professional activity in the field of information security and / or cybersecurity.
PLO 8 Research, develop and maintain information security and / or cybersecurity systems and tools at information facilities and critical infrastructure.
PLO 9 Analyze, develop and maintain the organization's information security and / or cyber security management system based on information security strategy and policy.
PLO 10 Ensure business / operational continuity, as well as identify vulnerabilities in information systems and resources, analyze and assess risks to information security and / or cybersecurity of the organization.
PLO 11 Analyze, control and ensure the effective functioning of the management system for access to information resources in accordance with established strategies and policies of information security and / or cybersecurity of the organization.
PLO 12 Research, develop and implement methods and measures to combat cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general.
PLO 13 Research, develop, implement and use methods and means of cryptographic and technical protection of information of business / operational processes, as well as analyze and evaluate the effectiveness of their use in information systems, information facilities and critical infrastructure.
PLO 14 Analyze, develop and maintain a system of audit and monitoring the effectiveness of information systems and technologies, business / operational processes in the field of information and / or cybersecurity in general.
PLO 15 To communicate one's own conclusions on information security and / or cybersecurity issues in a clear and unambiguous way, as well as the knowledge and explanations that substantiate them to staff, partners and others.
PLO 16 Make informed decisions on organizational and technical issues of information security and / or cybersecurity in complex and unpredictable conditions, including the use of modern methods and tools for optimization, forecasting and decision making.

PLO 17 Have the skills of autonomous and independent learning in the field of information security and / or cybersecurity and related areas of knowledge, analyze their own educational needs and objectively evaluate learning outcomes.	
PLO 18 Plan training, as well as monitor and supervise work with staff in the field of information security and / or cybersecurity.	
PLO 19 Select, analyze and develop suitable standard analytical, calculation and experimental methods of cybersecurity, develop, implement and support projects for the protection of information in cyberspace, innovation and intellectual property protection.	
PLO 20 Set and solve complex engineering and applied and scientific problems of information security and / or cybersecurity, taking into account the requirements of domestic and international standards and best practices.	
PLO 21 Use field, physical, and computer simulation techniques to study information security and / or cybersecurity processes.	
PLO 22 Plan and perform experimental and theoretical research, put forward and test hypotheses, choose appropriate methods and tools, perform statistical data processing, evaluate the reliability of research results, argue conclusions.	
PLO 23 Plan and perform experimental and theoretical research, put forward and test hypotheses, choose appropriate methods and tools, perform statistical data processing, evaluate the reliability of research results, argue conclusions.	
PLO 24 Know the vulnerabilities and methods of their application in various telecommunications technologies and SMART infrastructure. Be able to design secure (threat-sensitive) wired and wireless telecommunications and SMART systems.	
8 – Resource support for program implementation	
Staffing	Staffing of the educational and professional program consists mainly of the teaching staff of the Department of Information and Cyber Security. In accordance with their competence and experience, the teaching staff of the Department of Computer Science and Mathematics of the Faculty of Information Technologies and Management, the Department of Foreign Languages of the Faculty of Law and International Relations of the University is involved in the teaching of certain disciplines. The practice-oriented nature of the EPP provides for the broad participation of practitioners who correspond to the direction of the program, which strengthens the synergistic link between theoretical and practical training. The staffing of the EP meets the requirements set by the Licensing Conditions for Educational Activities.
Materially-technical provision	Teaching disciplines is carried out in classrooms of general and special purpose. Competence development centers are specially equipped with hardware and software, visual and methodical materials, namely: 1) "Center for Research of Technologies of Operation and Protection of Information and Communication Systems and Networks" with: training "Laboratory of Computer Networks and Cyber Security", training

	"Laboratory of Security of Information and Communication Systems" and training "Laboratory of Antivirus Protection"; 2) "Center for Research of Information Resources Protection Technologies" with: training "Laboratory of Information Assets Security" (training cyberfield) and training "Laboratory of Technical and Cryptographic Information Protection Systems"; 3) "Modeling and Programming Center", "Laboratory of Embedded Systems and 3D Modeling", etc. The areas of the premises used in the educational process meet the requirements of accessibility, sanitary norms, requirements of fire safety rules. There are all the necessary social and household infrastructure, dining room, cafeterias. The number of places in dormitories meets the requirements.
Information and training methodological provision	– Official website of Borys Grinchenko Kyiv University https://kubg.edu.ua/, which contains information about educational programs, educational, scientific and educational activities, structural units, admission rules, contacts, etc .; – Digital campus https: //digital.kubg.edu.ua/, which contains information about: all digital education services, digital science with access to various platforms; digital management of regulatory bases, registers, document flow; image and leadership; digital space with personal accounts and corporate mail; university infrastructure; – University e-learning system (Moodle); – services for organizing online classes: Google Meet (corporate) Google Chat, Google Hangouts, Google Classroom; – wireless access points to the Internet; – library, reading rooms; – electronic library, repository http://elibrary.kubg.edu.ua/; – access to electronic scientific databases Scopus, Web of Science, EBSCO, etc .; – curricula and work curricula; – schedule of the educational process; – working programs of academic disciplines; – internship programs; – methodical recommendations on writing and design of term papers, etc. – methodical recommendations on writing and registration of master's theses, etc.
9 – Academic mobility	
National credit mobility	-
International credit mobility	Agreements on student mobility have been concluded with universities in European countries and within the framework of the Erasmus + KAI program. 3 of them: Vilnius University (Lithuania), Constantine the Philosopher University in Nitra (Slovakia), Extremadura University (Spain). University of Silesia in Katowice (Poland), Jan Dlugosz Academy in Czestochowa (Poland), University of Ostrava (Czech Republic), University of Paris-Sorbonne (France), University of Lisbon (Portugal) and others.

Training of foreign applicants for higher education	According to the license, the training of foreigners and stateless persons is provided.

II. List of components of the educational and professional program and their logical sequence

2.1. List of the educational EP components

Component code	Component cipher	Components of the educational program (academic disciplines, course projects (works), practices, qualification work)	Number of credits	Final control form
1	2	3	4	5
Obligatory components of the EP				
EC 1	MD.01	Foreign language for professional purposes	4	credit
EC 2	MD.02	Organization of science and research	4	credit
EC 3	MD.03	Applied general theory of security systems	4	exam
EC 4	MD.04	Network and SMART infrastructure security technologies	7	exam, defense of term paper
EC 5	MD.05	Security technologies for wireless and mobile networks	7	credit
EC 6	MD.06	Web resource security technologies	6	exam
EC 7	MD.07	Security incident investigation technologies	6	credit
EC 8	MD.08	Applied aspects of penetration testing and ethical hacking	5	exam
EC 9	MP.01	Production practice (technological)	4,5	credit
EC 10	MP.02	Research practice	4,5	credit
EC 11	MP.03	Pre-diploma practice	6	credit
EC 12	MA.01	Preparation and defense of a master's thesis	6	defense
The total amount of required components			**64**	
Elective components of the EP (Annex 1)				
Elective block 1				
SC 1	SD.1.01	Monitoring, auditing and administration of secure IT systems and networks	7	exam
SC 2	SD.1.02	Network security software development and testing technologies	6	exam
SC 3	SD.1.03	Technologies for combating malicious code	5	exam
SC 4	SD.1.04	Mathematical methods of cryptography	4	credit
SC 5	SD.1.05	Methods of construction and analysis of cryptosystems	4	credit
		total	***26***	
Elective block 2 - Selection from the catalog of courses				
SC 1-5	SD 2.	the student chooses disciplines for the appropriate number of credits	26	credits, exams
		total	***26***	
The total amount of elective components			**26**	
TOTAL VOLUME OF THE EDUCATIONAL PROGRAM			**90**	

2.2. Structural and logical scheme

<table>
<tr><th colspan="2">1 course</th><th>2 курс</th></tr>
<tr><th>1 semester
30 cr.</th><th>2 semester
34,5 cr.</th><th>3 semester
25,5 cr.</th></tr>
<tr><td>Foreign language for professional purposes,
4 cr.</td><td></td><td></td></tr>
<tr><td>Organization of science and research,
4 cr.</td><td></td><td></td></tr>
<tr><td>Applied general theory of security systems,
4 cr.</td><td>Applied aspects of penetration testing and ethical hacking, 5 cr.</td><td>Research practice,
4,5 cr.</td></tr>
<tr><td>Network and SMART infrastructure security technologies, 7 cr.</td><td>Web resource security technologies,
6 cr.</td><td rowspan="2">Production practice (technological),
4,5 cr.</td></tr>
<tr><td>Security technologies for wireless and mobile networks, 7 cr.</td><td>Security incident investigation technologies,
6 cr.</td></tr>
<tr><td>Elective components,
4 cr.</td><td>Elective components,
13 cr.</td><td>Elective components,
9 cr.</td></tr>
<tr><td></td><td></td><td>Pre-diploma practice, 6 cr.</td></tr>
<tr><td></td><td colspan="2">Writing and defense of a master's thesis,
6 cr.</td></tr>
</table>

<table>
<tr><td colspan="3">Selective block 1</td></tr>
<tr><td colspan="2">Monitoring, auditing and administration of secure IT systems and networks,
7 cr.</td><td></td></tr>
<tr><td></td><td>Network security software development and testing technologies, 6 cr.</td><td>Technologies for combating malicious code, 5 cr.</td></tr>
<tr><td></td><td>Mathematical methods of cryptography
4 cr.</td><td>Methods of construction and analysis of cryptosystems,
4 cr.</td></tr>
<tr><td colspan="3">Selective block 2 – Selection of disciplines from the Catalog</td></tr>
<tr><td>Selective components,
4 cr.</td><td>Selective components,
13 cr.</td><td>Selective components,
9 cr.</td></tr>
</table>

III. Form of certification of applicants for higher education

Certification of applicants for higher education under the educational-professional program 125.00.02 "Security of information and communication systems" specialty 125 "Cyber Security" is carried out in the form of public defense of the master's thesis.

Certification is carried out openly and publicly.

The master's thesis is aimed at solving a complex problem of information security and / or cybersecurity and involves research and / or innovation.

Qualifying master's thesis is tested for plagiarism. Qualification work should not contain academic plagiarism, fabrication and / or falsification.

Qualifying master's thesis is published on the University website (in the repository). Publication of qualifying master's theses with limited access is carried out in accordance with the requirements of the legislation.

Implementation of the educational-professional program in full ends with the issuance of a document of the established standard to the graduate.

IV. Matrix of correspondence of program competencies to components of the educational program

Marks of learning outcomes and educational components	MD.01	MD.02	MD.03	MD.04	MD.05	MD.06	MD.07	MD.08	MP.01	MP.02	MP.03	MA.01
GC 1		+	+						+	+	+	+
GC 2		+								+	+	+
GC 3		+	+									+
GC 4		+							+	+	+	+
GC 5	+	+							+	+	+	+
GC 6	+								+	+	+	+
SC 1			+					+	+	+	+	+
SC 2		+		+	+	+	+	+	+	+	+	+
SC 3				+	+	+			+	+	+	+
SC 4			+				+		+	+	+	+
SC 5		+					+	+	+	+	+	+
SC 6				+	+				+	+	+	+
SC 7							+		+	+	+	+
SC 8				+	+	+	+	+	+	+	+	+
SC 9				+	+	+			+	+	+	+
SC 10		+	+						+	+	+	+
SC 11				+	+	+	+	+	+	+	+	+
SC 12				+	+	+			+	+	+	+

V. Matrix for supporting learning outcomes with relevant components of the educational program

Marks of learning outcomes and educational components	MD.01	MD.02	MD.03	MD.04	MD.05	MD.06	MD.07	MD.08	MP.01	MP.02	MP.03	MA.01
PLO 1	+											+
PLO 2		+										+
PLO 3		+	+							+	+	+
PLO 4			+						+	+	+	+
PLO 5		+					+	+	+	+	+	+
PLO 6				+			+	+	+	+	+	+
PLO 7		+	+						+	+	+	+
PLO 8				+	+	+			+	+	+	+
PLO 9				+	+	+			+	+	+	+
PLO 10				+			+		+	+	+	+
PLO 11					+	+			+	+	+	+
PLO 12							+		+	+	+	+
PLO 13			+		+		+		+	+	+	+
PLO 14				+	+	+			+	+	+	+
PLO 15	+	+							+	+	+	+
PLO 16			+						+	+	+	+
PLO 17	+	+	+						+	+	+	+
PLO 18		+							+		+	+
PLO 19		+	+	+	+	+			+		+	+
PLO 20			+	+	+	+	+	+		+	+	+
PLO 21		+	+				+	+		+	+	+
PLO 22		+	+							+	+	+
PLO 23			+	+		+	+	+	+	+	+	+
PLO 24				+	+		+		+	+	+	+

Annex 1 - ELECTIVE PART OF THE EDUCATIONAL PROGRAM

Students exercise the right to free choice of disciplines provided for in paragraph 15 of the first part of Article 62 of the Law of Ukraine "On Higher Education" at Borys Grinchenko Kyiv University in accordance with the Regulations on the procedure from November 25, 2016, № 642.

1. Elective block 1

To strengthen the practical orientation of professional competencies, students are offered a block of specialized disciplines. This block includes practical subjects in certain areas of information security and / or cybersecurity. All its components are included in the professional competencies and are described by the main learning outcomes.

Matrix of correspondence of program competencies components of the educational program of the sample unit

Marks of learning outcomes and educational components	SD.1.01	SD.1.02	SD.1.03	SD.1.04	SD.1.05
GC 1	+	+	+		
GC 3		+			
SC 1		+			
SC 2		+			
SC 3		+			
SC 4	+				
SC 5	+				
SC 6	+				
SC 8				+	+
SC 9	+				
SC 11	+				
SC 12	+	+			

Matrix for providing software learning outcomes relevant components of the educational program of the sample unit

Marks of learning outcomes and educational components	SD.1.01	SD.1.02	SD.1.03	SD.1.04	SD.1.05
PLO 3				+	+
PLO 4				+	+
PLO 5		+			
PLO 6		+			
PLO 11	+				
PLO 13				+	+
PLO 14	+				
PLO 19	+				
PLO 23		+			
PLO 24	+	+	+		

2. Elective block 2 - Choice from the course catalog

The choice of disciplines from the list (catalog of courses), taking into account their own needs and interests in future professional activities, allows students to deepen their knowledge and gain additional general and general professional competencies within related specialties and fields of knowledge and / or get acquainted with current research in other fields knowledge and expand or deepen knowledge in general competencies.