3. THE EDUCATIONAL PROGRAMME

Project Team Leader (Director of the Master's degree programme) - Yuliia Khokhlachova, PhD, Professor, Professor of the Department of Software Engineering and Cybersecurity.

3.1 The Educational Programme profile "Cybersecurity and information protection", subject area – F5 "Cybersecurity and information protection"

1 – GENERAL INFORMATION	
Full name of a HEI and a structural unit	State University of Trade and Economics Faculty of International Trade and Law Department of Software Engineering and Cyber Security
Higher Education Level and qualification name in the original language	Second (Master's) Cycle Qualification – Master's Degree in " Cybersecurity and information protection "
Field of Study	F Information technology
Subject Area	F5 Cybersecurity and information protection
Educational programme official name	Cybersecurity and information protection
Restrictions on Modes of Study	There are no restrictions
Compliance with the Higher Education Standard of the Ministry of Education and Science of Ukraine	Complies with the Higher Education Standard of the Ministry of Education and Science of Ukraine (Order No. 332 of 18.03.2021)
Diploma type and the Educational programme scope	Master's Degree Diploma, single, 90 ECTS credits, training period - 1 year 4 months
Accreditation Availability	Certificate of accreditation of the speciality No. 9819, valid until 01.07.2030, issued by the National Agency for Higher Education Quality Assurance.
Higher Education Cycle/Level	National Qualification Frameworks of Ukraine – level 7, FQ-EHEA – the second cycle, EQF-LLL –level 7
Prerequisites for Admission to the Educational Programme	Bachelor's degree (6th level of the NQF) or higher
Language(s) of training	Ukrainian
Programme validity period	Until the approval of the new edition of the educational programme
Internet address for permanent placement of the Educational programme description	https://knute.edu.ua/
2 – THE PURPOSE OF THE EDUCATIONAL PROGRAMME	
To provide applicants for higher education of the Second (Master's) Cycle with fundamental	

training in the subject area F5 "Cybersecurity and Information Protection", which is sufficient to solve a research and/or innovation problem in the field of information and/or cybersecurity in the field of economics.	
3 –EDUCATIONAL PROGRAMME CHARACTERISTICS	
Subject Area	- ***Object of study and activity***: - modern processes of research, analysis, creation and maintenance of information systems and technologies, other business operational processes at information facilities 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 activity facilities and critical infrastructures; - systems and complexes for the creation, processing, transmission, storage, destruction, protection and display of data (information flows); - information resources of various classes (including state information resources); - software and hardware and software (means) of cyber defence; - information security and/or cybersecurity management systems; - ***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 foundations of science-intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision-making, system analysis, complex systems, process modelling and optimisation, theory of mathematical statistics, cryptographic and technical information security, risk theory and other interdisciplinary theories and practices in the field of information security and/or cybersecurity. - ***Methods, techniques and technologies***: Methods, models, techniques and technologies for creating, processing, transmitting, receiving, destroying, displaying, protecting (cyber defence) information resources in cyberspace, as well as methods and models for developing and using application and specialised software to solve professional problems in the field of information security and/or cybersecurity. Technologies, methods and models of research, analysis, management and support of business/operational processes using a set of regulatory, legal, organisational and technical methods and means of protecting information resources in cyberspace. - ***Tools and equipment***: Means, devices, network equipment and environment, application and specialised software, automated systems and complexes for designing, modelling, operating, controlling, monitoring, processing, displaying and protecting data (information flows), as well as methods and models of risk theory and information resource management in the study and support of information activities in the field of information security and/or cybersecurity.
Educational Programme Orientation	Educational and professional; applied.

The Main Focus of the Educational Programme	Specialised education in the Field of Study "Information Technology", Subject Area "Cybersecurity and Information Protection". The programme is aimed at combining practice and science in the organisation, development and operation of complex components of cyberspace to ensure the information security of economic entities of the state economy, taking into account possible external cyber influences, possible threats and the level of development of technologies for protecting electronic communications systems. Keywords: security technologies for wireless and mobile networks, security technologies for Web resources, penetration testing, system vulnerability, information security management system of an economic entity, legal support for information security in economic systems, economic security of the State.
Educational Programme Features	The programme provides for the training of professionals capable of: modelling and forecasting possible cyber impacts on business entities and individuals; auditing electronic communications systems of business entities; applying regulatory documents and standards in developing measures to protect electronic communications systems of business entities.
4 – EMPLOYABILITY AND FURTHER EDUCATION OPPORTUNITIES FOR GRADUATES	
Employability	The specialist is able to perform professional work and hold positions defined by the National Classifier of Ukraine "Classifier of professions DK 003:2010": 2139.2 Cybersecurity infrastructure support specialist 2139.2 Specialist in technical protection of information 2139.2 Cybersecurity incident response specialist 2139.2 Cybersecurity infrastructure support specialist 2139.2 Specialist in assessment of information security measures (cybersecurity)) 2139.2 Specialist in cryptographic protection of information 2139.2 Specialist in cyber research and development of security systems 2132.2 Developer of information security systems 2359.2 Instructor-methodologist in information security 2139.2 Information technology auditor (cybersecurity)
Further Education Opportunities	Continuing education at the third (educational and scientific) level of higher education. Acquisition of additional qualifications in the adult education system.
5 – TEACHING AND ASSESSMENT	
Teaching and learning	A balanced combination of classroom studies (lectures, discussions, seminars, small group workshops, independent work with information sources, and teacher consultations), distance learning, and independent work based on problem-based, interactive learning and self-study.
Assessment	The assessment of students' learning outcomes is carried out in accordance with the Regulations on Assessment of Undergraduate and Postgraduate Students' Learning Outcomes at SUTE and includes the following control measures: current and final examinations, and certification. Current control is carried out during practical/laboratory classes and based on the results of independent work. It involves the assessment of students' theoretical training during seminars and acquired practical skills during laboratory/practical work.

	Final control is a control measure that involves establishing the compliance (measurement, evaluation) of the learning outcomes obtained by a person with the requirements of the Educational programme in terms of the relevant educational component, which is carried out at the university in the form of a credit and an exam. Students' learning outcomes at SUTE are assessed on a 100-point scale, where: 60-100 points – learning outcomes that entitle the student to obtain ECTS credits; 0-59 points – unsatisfactory learning outcomes that do not entitle the student to obtain ECTS credits.
6 - PROGRAMME COMPETENCES	
Integral competence	The ability of a person to solve research and/or innovation problems in the field of information security and/or cybersecurity.
General competences (GC)	GS-1. Ability to apply knowledge in practical situations. GS-2. Ability to conduct research at an appropriate level. GS-3. Ability to abstract thinking, analysis and synthesis. GS-4. The ability to evaluate and ensure the quality of the work performed. GS-5. Ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity). *GS -6. Ability to act socially responsible and socially conscious.* *GS -7. Ability to adapt and act in a new situation.* *GS -8. Ability to choose a communication strategy, work in a team.* *GS -9. The ability to communicate in the native language both orally and in writing, to communicate in a foreign language (mainly English) at a level that ensures effective professional activity.*
Special (professional, subject-specific) competences (SC)	SC1. The ability to reasonably apply, integrate, develop and improve modern information technologies, physical and mathematical models, as well as technologies for creating and using applied and specialized software to solve professional problems in the field of information security and/or cyber security. SC2 Ability to develop, implement and analyze regulatory documents, regulations, instructions and requirements of technical and organizational direction, as well as integrate, analyze and use the best global practices, standards in professional activities in the field of information security and/or cyber security. SC3. Ability to research, develop, and maintain information security and/or cyber security methods and tools at information activity and critical infrastructure facilities. SC4. The ability to analyze, develop and support the information security and/or cyber security management system of the organization, to form information security strategy and policy taking into account domestic and international standards and requirements. SC5. Ability to research, system analysis and ensure the continuity of business/operational processes in order to identify vulnerabilities of information systems and resources, analyze risks and determine their impact assessment in accordance with the established information security and/or cyber security strategy and policy of the organization. SC6. The ability to analyze, control and provide a management system for access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization.

	SC7. Ability to research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general. SC8. The ability to research, develop, implement and support methods and means of cryptographic and technical protection of information at objects of information activity and critical infrastructure, in information systems, as well as the ability to evaluate the effectiveness of their use, in accordance with the established strategy and policy of information security and/or cyber security of the organization. SC9. The ability to analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information security and/or cyber security of the organization as a whole. SC10. Ability to conduct scientific and pedagogical activities, plan training, monitor and support work with personnel, as well as make effective decisions on issues of information security and/or cyber security. SC*11. The ability to analyze electronic communications networks and counter actions that threaten the availability, integrity or confidentiality of such networks and services, as well as data stored, transmitted or processed, and related services, particularly in the economy.* *SC12. Ability to act as an internal consultant and advisor in your area of expertise.* *SC13. The ability to conduct research and experimental work on the procedure for scanning vulnerabilities and their recognition in security systems.*
7 –PROGRAMME LEARNING OUTCOMES	
	PLO1. Communicate freely in national and foreign languages, orally and in writing, to present and discuss the results of research and innovation, ensure business/operational processes and issues of professional activity in the field of information security and/or cyber security. PLO2. Integrate fundamental and specialized knowledge to solve complex information security and/or cyber security challenges in broad or multidisciplinary contexts. PLO3. Conduct research and/or innovation activities in the field of information security and/or cyber security, as well as in the field of technical and cryptographic protection of information in cyberspace. PLO4. Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and/or cyber security. PLO5. Critically consider the problems of information security and/or cyber security, including at the intersectoral and interdisciplinary level, in particular on the basis of understanding the new results of engineering and physical and mathematical sciences, as well as the development of technologies for creating and using specialized software. PLO6. Analyze and evaluate the security of systems, complexes and means of cyber protection, technologies for creating and using specialized software. PLO7. To justify the use, implement and analyze the best global standards, practices in order to solve complex problems of professional activity in the field of information security and/or cyber security.

	PLO8. Research, develop and support systems and means of information security and/or cyber security at objects of information activity and critical infrastructure. PLO9. Analyze, develop and support the organization's information security and/or cyber security management system based on information security strategy and policy. PLO10. Ensure the continuity of business/operational processes, as well as identify vulnerabilities of information systems and resources, analyze and assess risks for information security and/or cyber security of the organization. PLO11. Analyze, monitor and ensure the effective functioning of the information resources access management system in accordance with the established information security and/or cyber security strategy and policy of the organization. PLO12. Research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general. PLO13. Research, develop, implement and use methods and means of cryptographic and technical information protection of business/operational processes, as well as analyze and provide an assessment of the effectiveness of their use in information systems, objects of information activity and critical infrastructure. PLO14. Analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information and/or cyber security as a whole. PLO15. Clearly and unambiguously convey own conclusions on information security and/or cyber security issues, as well as the knowledge and explanations that justify them to staff, partners and others. PLO16. Make informed decisions on organizational and technical issues of information security and/or cyber security in complex and unpredictable conditions, including using modern methods and means of optimization, forecasting and decision-making. PLO17. Have the skills of autonomous and independent learning in the field of information security and/or cyber security and related fields of knowledge, analyze one's own educational needs and objectively evaluate the results of training. PLO18. Plan training, as well as accompany and supervise work with personnel in the direction of information security and/or cyber security. PLO19. Choose, analyze and develop suitable typical analytical, calculation and experimental methods of cyber protection, develop, implement and support the project on the protection of information in cyberspace, innovative activities and protection of intellectual property. PLO20. Set and solve complex applied engineering and scientific problems of information security and/or cyber security, taking into account the requirements of domestic and international standards and best practices. PLO21. Use the methods of natural, physical and computer modeling to study processes related to information security and/or cyber security.

	PLO22. Plan and carry out experimental and theoretical research, put forward and test hypotheses, choose suitable methods and tools for this, carry out statistical processing of data, evaluate the veracity of research results, argue conclusions. PLO23. Justify the selection of software, equipment and tools, engineering technologies and processes, as well as their limitations in the field of information security and/or cyber security based on current knowledge in related fields, scientific, technical and reference literature and other available information. PLO*24. Make informed decisions and take appropriate technical and organizational measures to ensure the security of electronic communication networks and services in order to guarantee the integrity of own electronic communication networks, the continuity of the provision of electronic communication services, and the prevention of unauthorized access to electronic communication networks.* *PLO25. Perform the duties of an internal consultant/advisor in the technical field and the field of copyright in relation to electronic media.* *PLO26. Communicate with managers of different levels (interpersonal communication, accessibility, ability to effectively perceive the speaker's language, adjust the style and language of the speech according to the audience).* *PLO27. Conduct security system scanning of information resources for vulnerabilities.* *PLO28. Apply the principles of information security - preservation of confidentiality, integrity and availability.*
8 – RESOURCE SUPPORT FOR PROGRAMME IMPLEMENTATION	
Staffing	Fully complies with the licensing requirements for educational activities. The educational and professional programme 'Cybersecurity and information protection' is implemented by academic staff with scientific degrees and/or academic titles who meet the requirements of the current legislation of Ukraine and have a sufficient level of scientific and professional qualifications. Practitioners, representatives of professional associations and foreign partners are also involved in the educational process. All academic staff undergo training/professional development every five years.
Material and technical support	Fully complies with the Licensing Requirements for Educational Activities. For the convenience of higher education students, there is a corporate distance learning system and an automated educational process management system called 'MIA: Education'. The university has modern computer classrooms with specialised software, a Business Simulation Training and Research Centre and a Smart Library. All conditions for the education of persons with disabilities have been created. SUTE social infrastructure is available.
Information and educational-methodological support	An ECTS Information Package is developed for each educational programme at the university. Each student can view and create his/her individual plan, view the curriculum, grades obtained in disciplines, class schedule, and communicate with participants in the educational process through a personal account in the MIA: Education automated information system.

	Course summaries, course outlines, syllabi and assessment criteria for educational components are posted on the corporate distance learning platform. The university's electronic repository provides full-text access to SUTE scientific and educational literature, manuscripts of qualification works and theses for obtaining academic degrees. For the convenience of higher education students, the university has developed a Catalogue of Academic Disciplines, according to which students have the right to choose elective educational components.
9 – ACADEMIC MOBILITY	
National credit mobility	National credit mobility is implemented within the framework of memoranda of cooperation concluded between SUTE and other higher education institutions (research institutions) in Ukraine under the law.
International credit mobility	The university has signed cooperation agreements between SUTE and foreign higher education institutions, which provide for partnership exchanges and training of students under international programmes and projects within the Erasmus+ programme. Organisation of credit mobility (except for the 1st year) for bachelors. mobility agreement between SUTE and the Slovak University of Technology (Bratislava): Erasmus+ Learning Agreement Student Mobility for Studies International Mobility (KA171). The academic mobility agreement is valid from 2024 to 2027.
Foreign higher education students training	It is carried out in accordance with the requirements of the current legislation.

3.2. LIST OF THE EDUCATIONAL PROGRAMME COMPONENTS AND THEIR LOGICAL SEQUENCE

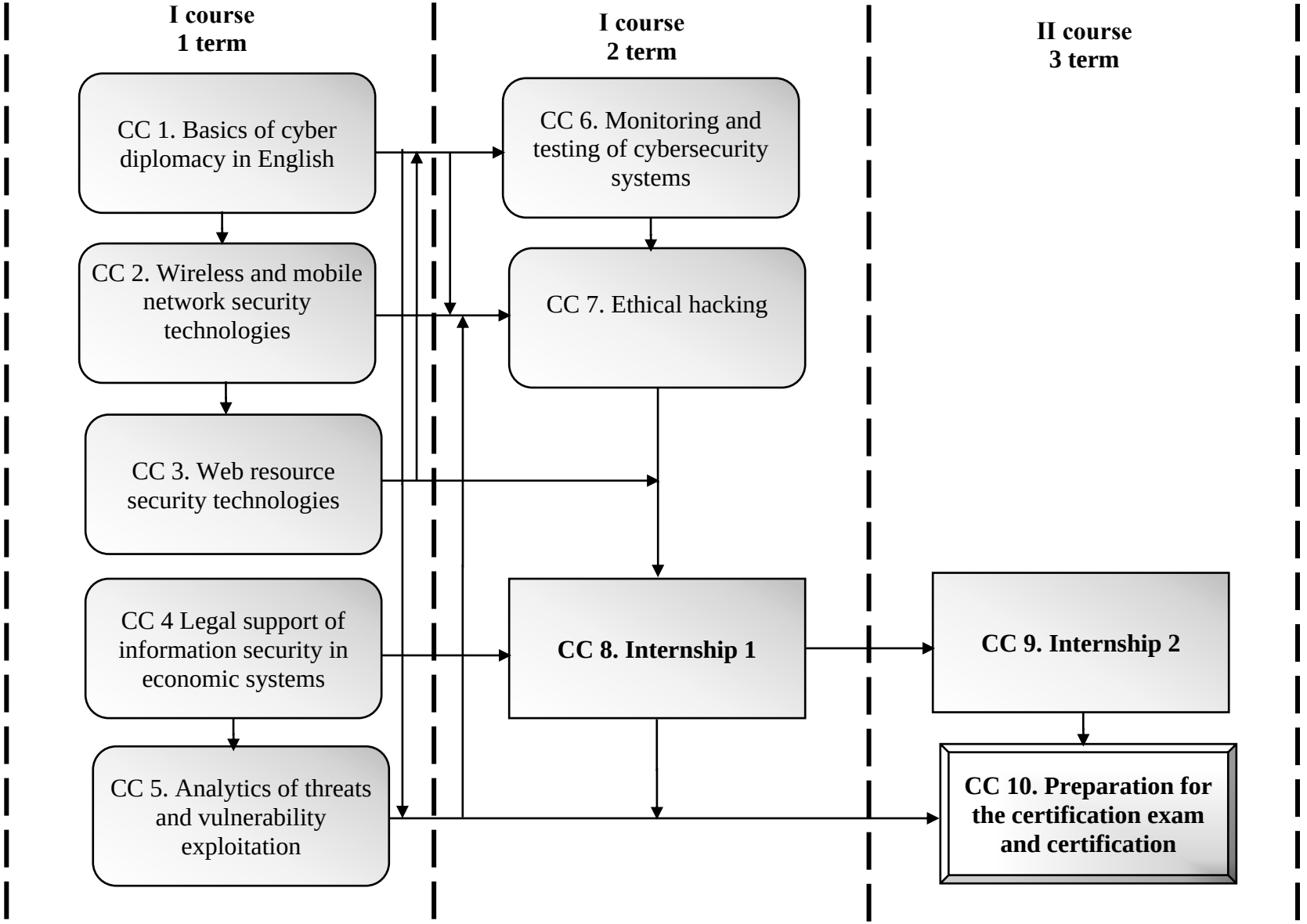
3.2.1 LIST OF EP COMPONENTS

Code	Educational programme components	The number of credits	Form of control
1	2	3	
EP Compulsory Components			

CC 1.	Basics of cyber diplomacy in English	6	Exam
CC 2.	Wireless and mobile network security technologies	6	Exam
CC 3.	Web resource security technologies	6	Exam
CC 4.	Legal support of information security in economic systems	6	Exam
CC 5.	Analytics of threats and vulnerability exploitation	6	Exam
CC 6.	Monitoring and testing of cybersecurity systems	6	Exam
CC 7.	Ethical hacking	6	Exam
CC 8.	Internship 1	12	Credit
CC 9.	Internship 2	3	Credit
CC 10.	Preparation for the certification exam and certification	9	Exam
Total Volume of Compulsory Components:		**66**	
EP Elective Components			
EC1.	Educational Component 1	6	Exam
EC2.	Educational Component 2	6	Exam
EC3.	Educational Component 3	6	Exam
EC4.	Educational Component 4	6	Exam
Total Volume of Elective Components		**24**	
TOTAL EP VOLUME:		**90**	

Higher education students choose their elective disciplines through the personal account of the portal "MIA: Education". Descriptions of the disciplines and their prerequisites are available in the SUTE Catalogue of Disciplines

2.2 Structural and logical scheme of EP



3. FORMS OF ATTESTATION OF HIGHER EDUCATION STUDENTS

Attestation is carried out in the form of a public defence of a qualification work. The qualification work should provide for the solution of a complex specialised task or problem in the field of modern marketing, which involves research and/or innovation and is characterised by uncertainty of conditions and requirements. The qualification work must not contain academic plagiarism, including incorrect textual borrowings, fabrication and falsification. The qualification work must be published on the official website of the higher education institution, its subdivision or placed in its repository. The publication of qualification papers containing information with restricted access is carried out in accordance with the requirements of the current legislation.

4. MATRIX OF CORRESPONDENCE BETWEEN PROGRAM COMPETENCIES AND COMPULSORY COMPONENTS OF THE EDUCATIONAL PROGRAMME

Components / Competencies	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10
GC-1.	+	+	+	+	+	+	+	+	+	+
GC -2.		+	+	+	+		+			+
GC -3.	+				+	+	+			+
GC -4.			+		+	+		+	+	
GC -5.	+	+		+	+		+			
GC -*6.*	+			+	+		+			
GC -*7.*	+			+	+			+	+	
GC -*8.*	+			+				+	+	
GC -*9.*	+							+	+	+
SC1.		+	+	+	+	+	+	+	+	+
SC 2.	+	+	+	+	+	+	+	+	+	+
SC 3.		+		+	+	+	+	+	+	+
SC 4.	+	+		+		+	+	+	+	+
SC 5.	+	+	+			+	+	+	+	+
SC 6.			+					+	+	+
SC 7.			+		+			+	+	+
SC 8.						+		+	+	+
SC 9.		+				+	+	+	+	+
SC 10.	+			+			+	+	+	+
SC 11.		+			+	+		+	+	+
SC 12.	+	+	+	+	+	+	+	+	+	+
SC 13.		+	+		+	+	+	+	+	+

5. MATRIX OF CORRELATION BETWEEN PROGRAM LEARNING OUTCOMES AND COMPULSORY COMPONENTS OF THE EDUCATIONAL PROGRAMME

Components / Programme learning outcomes	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10
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		+				+		+	+	+
PLO 25	+	+	+	+	+	+	+	+	+	+
PLO 26	+			+				+	+	+
PLO 27		+	+		+	+	+	+	+	+
PLO 28		+	+		+	+	+	+	+	+

LIST OF RECOMMENDED ELECTIVE COMPONENTS

Code	EDUCATIONAL PROGRAMME COMPONENTS	The number of credits
EC 1.	UI/UX design in English	**6**
EC 2.	Data storage administration and protection	**6**
EC 3.	Mobile application security	**6**
EC 4.	Security of Internet of Things technologies	**6**
EC 5.	Information technologies in the system of ensuring economic security of the state	**6**
EC 6.	Legal regulation of business security	**6**