LIMITED LIABILITY COMPANY
"HIGHER EDUCATIONAL INSTITUTION
"AMERICAN UNIVERSITY KYIV"

APPROVED
By the Academic Council
LLC "Higher Educational Institution
"American University Kyiv"
Protocol N 10 dated 30.06.2026

Put into effect
By order of the Rector
LLC "Higher Educational Institution
"American University Kyiv"
N 88-OD dated 30.06.2026

EDUCATIONAL AND PROFESSIONAL PROGRAM "CYBERSECURITY"

Higher education level:	First (bachelor's)
Higher Education Degree:	Bachelor
Field of knowledge:	F Information Technology
Specialty:	F5 Cybersecurity and information protection

Kyiv, 2026

1. Preamble

Developed in accordance with the standard of higher education of Ukraine in the specialty 125 Cybersecurity and Information Protection for the first (bachelor's) level of higher education, approved by the Order of the Ministry of Education and Science of 04.10.2018, No 1074 (as amended by the Order of the Ministry of Education and Science of 29.10.2024, No 1547)

Composition of the development group:

Surname, first name, patronymic	Academic degree, academic title, position
Development team:	
Oliynyk Andriy Stepanovych	Doctor of Physical and Mathematical Sciences, Professor, Professor of the Department of Information Technologies
Didkovska Maryna Vitalievna	Candidate of Technical Sciences, Associate Professor of the Department of Information Technologies
Tytenko Serhii Volodymyrovych	Candidate of Technical Sciences, Associate Professor of the Department of Information Technologies

REVIEWED AND APPROVED:
- at a meeting of the Department of Information Technologies of LLC "Universities "American University Kyiv" Protocol N 2 dated February 2, 2026.

2. General characteristics

Full official name of the institution	Limited Liability Company "Higher Educational Institution "American University Kyiv"
Full name of the structural unit	EPAM Faculty of Digital Technologies
Higher education level	First (bachelor's)
Higher education degree	Bachelor; Bachelor of Science in Cybersecurity and Information Security
Name of the field of knowledge	F Information Technology
Name of specialty	F5 Cybersecurity and Information Protection
Official name of the educational and professional program	Cybersecurity
Type of Diploma and Scope educational and professional program	Bachelor's degree, single, 240 ECTS credits
Availability of accreditation	OPP is not accredited
Language(s) of instruction	Ukrainian, English
Forms of education	Full-time (daytime, evening)
Term of education	3 years 10 months
Internet address of permanent placement of the description of the educational and professional program	https://auk.edu.ua
Cycle/Level	NQF – Level 6, FQ-EHEA – First Cycle, EQF LLL – Level 6
Requirements for the level of persons who can start training in the educational field program	3rd or higher level of the NQF of Ukraine
Requirements for the level of persons who can start training in the educational field program	Complete general secondary education
Purpose of the educational program	Training of highly qualified specialists who are able to combine general and professional knowledge and skills, communication skills, autonomous activity and responsibility, who have modern standards and technologies for creating, analyzing and maintaining information security systems, quickly adapt to new business conditions, are able to work in teams responsible for cybersecurity and manage such teams.

Subject area	*Object:* cybersecurity and information protection technologies; cybersecurity and information protection management processes; objects of information activity, including information and information and communication systems, information resources and technologies. *The purpose of the training* is to train specialists who are able to use and implement cybersecurity and information protection technologies and solve complex problems in the field of cybersecurity and information protection. *Theoretical content of the subject area*: principles, concepts, theories of protection of vital interests of a person, society, state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely identification, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace. *Methods, techniques and technologies*: methods, techniques and technologies for solving theoretical and practical problems of cybersecurity and information protection. *Tools and equipment*: tools, devices, network equipment, applied and specialized software, information systems and complexes for design, modeling, control, monitoring, storage, processing, display and protection of data (information flows).
Orientation of the educational and professional program	Bachelor's Educational and Professional Program. The main orientation of the program is practical professional activity; The focus of the program is applied, practical.
The main focus of the educational and professional program and specialization (if any)	*General education:* activities for the organization and management in the field of cybersecurity, information protection and ensuring the stability of information systems. *Special education:* activities for the organization and management of solving complex specialized tasks or practical problems in the field of cybersecurity and information protection, characterized by complexity and uncertainty of conditions, using the theory and methods of information technology, cryptographic and technical protection. *Keywords* cybersecurity, information protection, information security, threat monitoring, cryptography, countering cyberattacks, technical information protection, risk management.
Features of the educational and professional program	The program is unique because it is based on the experience of forming and teaching similar programs at the world-class university Arizona State University (ASU). The program is focused on attracting the best specialists in the field to the educational process: practitioners and experts of domestic and American higher education institutions, attracting students to international academic mobility programs and double degree programs in teaching in Ukrainian and English.
Employment of graduates	Professional activity in the following titles of work: specialist in cryptographic information protection, specialist in security issues

	(information and communication technologies), specialist in maintaining cyber defense infrastructure, specialist in responding to cybersecurity incidents, specialist in testing security systems and information protection, specialist in technical information protection, specialist in the field of information protection, vulnerability assessment analyst in accordance with the Classifier of Professions DK 003:2010. The rights of graduates to employment are not limited.
Further training	Bachelors can continue their education at the second (master's) level of higher education, as well as improve their qualifications and receive additional postgraduate education.
3. Teaching and Assessment	
Teaching and learning	Learning approaches: student-centered learning; self-study; Professionally-oriented training. A combination of traditional and non-traditional teaching methods: lectures, including with the participation of practitioners; practical classes, seminars, presentations; solving problems, solving computational problems; conducting a consultation with teachers. A special type of classes is the format of group classes, during which students receive a business case and form architectural solutions for software development for it (architectural executions).
Assessment	Assessment methods – exams, tests, practice, essays, presentations. The educational program provides for formative assessment (written and oral comments and instructions of teachers in the learning process, the formation of self-assessment skills, the involvement of students in the evaluation of each other's work) and summative assessment (written exams in academic disciplines, assessment of current work during the study of individual educational components (written essays, presentations, testing, analytical and research works), defense of practice reports, public defense qualification work) assessment, which determines the level of achievement of the expected program learning outcomes
4. List of competencies of the graduate	
Integral Competence (IC)	Ability to solve complex specialized tasks and practical tasks in the field of cybersecurity and information protection.
General Competence (GC)	ZK 01. Ability to apply knowledge in practical situations. ZK 02. Knowledge and understanding of the subject area and understanding of professional activities. ZK 03. Ability to communicate in the state language both orally and in writing. ZK 04. Ability to communicate in a foreign language. ZK 05. Ability to learn and master modern knowledge. ZK 06. Ability to realize one's rights and obligations as a member of society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.

	ZK 07. Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty. ZK 08. Ability to preserve and multiply moral, cultural, scientific values and achievements of society on the basis of understanding the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, technology and technology, to use various types and forms of physical activity for active recreation and leading a healthy lifestyle.
Special Competence (SC)	SK 01. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in professional activities. SK 02. Ability to use information technologies, modern methods and models of cybersecurity and information security systems. SK 03. Ability to ensure the continuity of business processes in accordance with the established cybersecurity and information protection policy. SK 04. Ability to ensure the protection of information in information and information and communication systems in accordance with the established policy of cybersecurity and information protection. SK 05. Ability to restore the functioning of information and information and communication systems after the implementation of threats, cyberattacks, failures and failures of various classes and origins. SK 06. Ability to implement and ensure the functioning of complex information security systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.) SK 07. Ability to carry out professional activities based on the implemented information and cybersecurity management system. SC 08. Ability to apply methods and means of cryptographic protection of information on objects of information activity. SK 09. Ability to apply methods and means of technical protection of information at the objects of information activity. SC 10. Ability to monitor information processes, analyze, identify, assess possible vulnerabilities and threats to the information space and information resources in accordance with the established information security policy. SC 11. The ability to use artificial intelligence methods and tools to automate the processes of detection, analysis, and prevention of cyber threats, as well as to ensure the security of machine learning systems themselves.
5. The normative content of the training of higher education applicants, formulated in terms of learning outcomes	

Program Learning Outcomes (RN)	RN 01. To communicate fluently in the state language orally and in writing in the performance of professional duties. RN 02. Communicate in a foreign language in order to ensure the effectiveness of professional communication. PH 03. Apply the principle of inadmissibility of corruption and any other manifestations of dishonesty in professional activities. RN 04. Organize their own professional activity, choose and use the best methods and ways to solve complex specialized tasks and practical problems in professional activity, evaluate their effectiveness. RN 05. Analyze, argue, make decisions when solving complex specialized tasks and practical tasks in professional activity, which are characterized by complexity and incomplete certainty of conditions, be responsible for the decisions made. PH 06. Adapt to new conditions and technologies of professional activity, predict the final result. RN 07. Apply and adapt the theories of information and coding, mathematical statistics, numbers, cryptography and steganography, signal processing and transmission, etc., principles, methods, concepts of cybersecurity and information protection in education and professional activities. PH 08. Apply knowledge and understanding of mathematics and physics in professional activities, formalize the problems of the subject area of cybersecurity and information protection, formulate their mathematical formulation and choose a rational method of solution. RN 09. Know and apply the legislation of Ukraine and international requirements, practices and standards in order to carry out professional activities in the field of cybersecurity and information protection. PH 10. To use modern information technologies, methods and models of cybersecurity and information security systems for the implementation of professional activities. PH 11. Plan the preparation and ensure the continuity of business processes in organizations in accordance with the established cybersecurity policy, taking into account the requirements for information protection. PH 12. Apply methods and means of information protection in information and information and communication systems in accordance with the established information security policy. PH 13. Implement, configure, accompany and support the functioning of software and hardware complexes and systems of cybersecurity and information protection as necessary procedures for the functioning of information and information and communication systems and/or the infrastructure of the organization as a whole.

	PH 14. Solve the problems of managing the processes of restoring the normal functioning of information and information and communication systems using redundancy procedures in accordance with the established security policy and ensure the functioning of special software for the protection and recovery of information. PH 15. Collect, process, store, analyze critical data to prove the implementation of cyber threats, analyze and investigate a cyber incident in order to promptly restore the functioning of the information system. PH 16. Solve the problems of implementation and maintenance of complex information security systems in information systems; PH 17. To ensure the functioning of the organization's cybersecurity and information protection management system, including personnel and management of the consequences of the implementation of threats to information security in crisis situations, based on the implementation of quantitative and qualitative risk assessment procedures. PH 18. To analyze, apply methods and means of cryptographic protection of information at the objects of information activity. PH 19. Solve problems related to the organization and control of the state of cryptographic protection of information, in particular in accordance with the requirements of regulatory documents. PH 20. Identify threats of creating technical channels of information leakage at the objects of information activity; to implement means and measures of technical protection of information from leakage through technical channels, to carry out maintenance and control of the condition of hardware means of information protection and complexes of technical protection of information. PH 21. Implement, support, analyze the effectiveness of systems for detecting unauthorized access, actions with information in the information system, vulnerabilities, possible threats to the information space and information resources, and use protection complexes to ensure the necessary level of information security in information systems. PH 22. Apply machine learning algorithms and data mining techniques to detect anomalies, predict cyber threats, and automate incident response processes in information and communication systems.
6. Form of attestation of applicants for higher education	
Forms of attestation of higher education applicants	Certification is carried out in the form of the Unified State Qualification Exam (USCI). The Unified State Qualification Exam provides for the assessment of the achievements of learning outcomes determined by this standard.
Requirements for the USCI	The Unified State Qualification Exam provides for the assessment of the achievements of learning outcomes determined by the standard of

	higher education of Ukraine in the specialty *Cybersecurity and Information Protection* for the first (bachelor's) level of higher education.
7. Resource provision and academic mobility	
Staffing	Scientific and pedagogical workers who ensure the implementation of the educational and professional program have scientific degrees and/or academic titles; in terms of qualifications, they correspond to the profile and direction of the disciplines taught; have the necessary experience of scientific, scientific and pedagogical and practical work experience. Professionals with experience in research, management, innovation, creative and professional work, who have successful business results and relevant education, are also involved in teaching academic disciplines.
Material and technical Provision	The educational process according to the educational program takes place in specialized classrooms equipped with audiovisual equipment and the necessary technical means. The areas and material and technical support of all departments involved in the provision of the educational process under the program are used. Library, including reading room. The library catalog of printed educational publications is available at the link https://opac.auk.edu.ua/. However, the availability of educational, research and reference literature for BSE educational programs is based not only on printed publications, but also on licensed electronic resources. The library provides its users with free access to licensed content of the world's best IT and business resources, which is provided 24/7. Recommended sources from the syllabuses of educational components are fully provided by the following platforms: Research4Life, ProQuest Ebook Central (Part of Clarivate), O'Reilly Media, JSTOR, ACM(DL). Internet access.
Informational and educational support	The official website of the educational institution https://auk.edu.ua contains information about educational programs, educational, scientific and organizational activities, structural units, admission rules, contacts, etc. Applicants for higher education under the educational program can use the databases of the information and reference system "ProQuest", the network "Cengage PH", access to "SAGE Publication", library software "Koha" and "ProQuest". Access to all library bases is provided through students' university accounts. Students and teachers can use the library fund and use methodological material prepared by teachers and posted in LMS Canvas: materials from textbooks, presentations on lectures, methodological instructions for practical, seminar classes, individual tasks, etc. Methodological material can be provided both in printed form and in electronic form. The AUC Library provides its users with free access to licensed content of the world's best resources in the field of IT and business, which is

	provided 24/7. Recommended sources from the syllabuses of educational components are fully provided by the following platforms: Research4Life, ProQuest Ebook Central (Part of Clarivate), O'Reilly Media, JSTOR, ACM(DL). Access to the databases of scientific periodicals, which are necessary for conducting individual research, is free for students and teachers of AUC and is possible from any digital device. This is about 500 titles of journals in the thematic area of the archive mostly before 1995 (Research4Life, JSTOR) and 177,500 journal articles on scientific and technical topics in the ACM(DL) database. The methodological material is periodically updated and adapted to the goals of the educational program. system for remote monitoring of academic integrity and proctoring of exams and milestone unit control (current testing) LockDown Browser, Respondus Monitor. Full online access of students and teachers to the family of modern IntelliJ IDEA IDEs.
National Credit Mobility	National credit mobility can be carried out in accordance with the agreements of the University with other institutions of higher education of Ukraine and implemented by applicants for higher education under the educational program in higher education institutions (scientific institutions) – partners of the university within Ukraine.
International credit mobility	International credit mobility can be implemented by applicants for higher education in educational programs in accordance with the agreements concluded with partners of the University outside Ukraine. International academic mobility is implemented on the basis of partnership with the main partner of the university – Arizona State University.
Training of foreign applicants for higher education	It is assumed.

8. Requirements for the presence of an internal Quality Assurance of Higher Education

A higher education institution should have a system for ensuring the quality of educational activities and the quality of higher education (internal quality assurance system), which provides for the implementation of the following procedures and measures:

1) determining the principles and procedures for ensuring the quality of higher education;

2) monitoring and periodic review of educational programs;

3) annual assessment of higher education applicants, scientific, pedagogical and pedagogical staff of the higher education institution and regular publication of the results of such assessments on the official website of the higher education institution, on information stands and in any other way;

4) provision of advanced training of pedagogical, scientific and scientific-pedagogical workers;

5) ensuring the availability of the necessary resources for the organization of the educational process, including independent work of students, for each educational program;

6) ensuring the availability of information systems for effective management of the educational process;

7) ensuring the publicity of information about educational programs, higher education degrees and qualifications;

8) ensuring compliance with academic integrity by employees of higher education institutions and higher education applicants, including the creation and maintenance of an effective system for preventing and detecting academic plagiarism;

9) other procedures and measures. The system of ensuring the quality of educational activities and the quality of higher education by a higher education institution (internal quality assurance system) at the request of the higher education institution is evaluated by the National Agency for Quality Assurance of Higher Education or independent institutions for evaluation and quality assurance of higher education accredited by it for its compliance with the requirements for the quality assurance system of higher education, which are approved by the National Agency.

9. Explanatory note

Table 1/Table 1

List of components of the educational and professional program

Code/ Sode	The educational component (academic discipline, types of practice, qualification work)	A few hundred chalks - Number of ECTS credits	Final control form
1. Cycle of general training		**33**	
GEN 101	AUK Experience and Academic English	6	Differentiated scoring
GEN 109	Спортивні студії/ Sport Studios	2	Differentiated scoring
GEN 110	Українські студії / Ukrainian Studios	2	Differentiated scoring
GEN 120	Introduction to Ethics/ Introduction to Ethics	6	Exam
GEN 250	Базова загальновійськова підготовка (теоретичний курс) **/ Basic Military Training (Theoretical Part)**	3	Differentiated scoring

GEN 0	Вибірковий альтернативний ОК*** / Elective Alternative Course***		
GEN 300	Суспільство та право / Society and Law	2	Differentiated scoring
SDT 150	Higher Mathematics for Engineers I/ Calculus for Engineers and	6	Exam
SDT 151	Higher Mathematics for Engineers II/ Calculus for Engineers II	6	Exam
2. Cycle of core professional training		**132**	
SDT 100	Principles of programming/ Principles of Programming	6	Exam
SDT 101	Object-Oriented Programming and Data Structures / Object-Oriented Programming and Data Structures	6	Exam
SDT 105	Основи комп'ютерних систем та мова асемблера/ Computer Systems Fundamentals and Assembly Language	6	Exam
SDT 107	Principles of programming languages/ Principles of Programming Languages	6	Exam
SDT 111	Introduction to Cybersecurity/ Introduction to Cybersecurity	6	Exam
SDT 112	Security and Management Policy/ Security Policy and Governance	6	Exam
SDT 113	Mathematical Foundations of Cryptography / Mathematical Foundations of Cryptography	6	Exam
SDT 202	Design and Analysis of Data Structures and Algorithms	6	Exam
SDT 222	Теорія інформації та кодування/ Theory of Information and Coding	6	Exam
SDT 223	Applied cryptology and steganography	6	Exam
SDT 250	Дискретні математичні структури/ Discrete Mathematical Structure	6	Exam
SDT 252	Ймовірність і статистика для інженерії/ Probability and Statistics for Engineering	6	Exam
SDT 302	Операційні системи та системне програмування/ Operation Systems and Systems Programming	6	Exam
SDT 303	Принципи розподілених інформаційних систем / Principles of Distributed Software Systems	6	Exam
SDT 304	Проєктування безпечних інформаційних систем / Engineering Secure Software Systems	6	Exam
SDT 305	Principles of database management/ Principles of Database Management	6	Exam
SDT 312	Комп'ютерні мережі та інформаційна безпека/ Computer Networks and Information Security	6	Exam
SDT 314	Розробка програмного забезпечення та шаблони/ Software Design and Patterns	6	Exam
SDT 315	Вступ до штучного інтелекту/ Introduction to Artificial Intelligence	6	Exam
SDT 316	Основи хмарних технологій та DevSecOps/ Cloud and DevSecOps Fundamentals	6	Exam
SDT 421	Комплексні системи інформаційної безпеки/ Complex Information Security Systems	6	Exam
SDT 423	Системи технічної безпеки інформації/ Systems of Technical Information Security	6	Exam
1. **Cycle of core practical training**		**6**	
SDT 491	BCYB Internship	6	Differentiated scoring
5. Attestation of higher education students		**6**	

SDT 490	Єдиний державний кваліфікаційний іспит/ Unified State Qualification Exam		Exam
Загальна кількість кредитів ЄКТС обов'язкових компонентів / Total ECTS Credits of Core Courses		**165**	
5. Cycle of general elective training Catalog 1		**18**	
BSE 1.1	Discipline 1 Catalog 1/ Course 1 Catalog 1	6	Exam
BSE 1.2	Discipline 2 Catalog 1/ Course 2 Catalog 1	6	Exam
BSE 1.3	Discipline 3 Catalog 1/ Course 3 Catalog 1	6	Exam
6. Cycle of professional elective training Catalog 2		**60**	
BSE 2.4	Course 4 Catalog 2 / Course 4 Catalog 2	6	Exam
BSE 2.5	Course 5 Catalog 2 / Course 5 Catalog 2	6	Exam
BSE 2.6	Course 6 Catalog 2 / Course 6 Catalog 2	6	Exam
BSE 2.7	Course 7 Catalog 2 / Course 7 Catalog 2	6	Exam
BSE 2.8	Course 8 Catalog 2 / Course 8 Catalog 2	6	Exam
BSE 2.9	Course 9 Catalog 2 / Course 9 Catalog 2	6	Exam
BSE 2.10	Course 10 Catalog 2 / Course 10 Catalog 2	6	Exam
BSE 2.11	Discipline 11 Catalog 2 / Course 11 Catalog 2	6	Exam
BSE 2.12	Discipline 12 Catalog 2 / Course 12 Catalog 2	6	Exam
BSE 2.13	Discipline 13 Catalog 3 / Course 13 Catalog 3	3	Exam
Total ECTS Credits of Elective Courses		**75**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ/ THE TOTAL SCOPE OF THE EDUCATION PROGRAM		**240**	

***** The choice of academic disciplines and the creation of an individual educational trajectory is regulated by the Law of Ukraine "On Higher Education" and internal regulatory documents. Elective components are selected by higher education applicants from the university-wide catalog and the catalog of alternative elective disciplines/

The choice of academic disciplines and the creation of an individual educational trajectory is regulated by the Law of Ukraine "On Higher Education" and internal regulatory documents. Elective components are selected by higher education applicants from the university-wide catalog and the catalog of alternative elective disciplines.

Table 2

General distribution of ECTS credits by blocks and cycles

Preparation cycle	**Number of ECTS credits / % of the total number of ECTS credits**		
	Compulsory educational components	**Selective educational components**	**Total**
General training cycle	33/13,75%	18/7,5%	51/21,25%
Cycle of professional training in the specialty of which. - Practical training - Final certification	132/55%	57/23,75%	189/78,75%
Total	**165/68,75%**	**75/31,25%**	**240/100%**

List of regulatory documents on which the educational and professional program is based

1. Law of Ukraine of 01.07.2014 No 1556-VII "On Higher Education" [Access mode: http://zakon5.rada.gov.ua/laws/show/2145-19]; - Law of Ukraine of 05.09.2017 "On Education" – [Access mode: http://zakon5.rada.gov.ua/laws/show/2145-19];

2. Resolution of the Cabinet of Ministers of Ukraine of 29.04.2015 No 266 "On approval of the list of fields of knowledge and specialties for which training of higher education applicants is carried out" [Access mode: http://zakon4.rada.gov.ua/laws/show/266-2015-p];

3. Resolution of the Cabinet of Ministers of Ukraine dated 30.12.2015 No 1187 "On Approval of Licensing Conditions for Conducting Educational Activities" [Access mode: http://zakon4.rada.gov.ua/laws/show/1187-2015-p/page] - Resolution of the Cabinet of Ministers of Ukraine dated 23.11.2011 No 1341 "On approval of the National Qualifications Framework" [Access mode: http://zakon4.rada.gov.ua/laws/show/1341-2011-p];

4. National Classifier of Ukraine: "Classification of Economic Activities" DK 009: 2010 [Access mode: http://www.ukrstat.gov.ua/];

5. National Classifier of Ukraine: "Classifier of Professions" DK 003: 2010DK 003:2010 [Access mode: http://www.dk003.com];

6. Order of the Ministry of Education and Science of Ukraine dated 04.10.2018, No. 1074 (as amended by the Order of the Ministry of Education and Science of Ukraine dated 29.10.2024, No. 1547) "On Approval of the Standard of Higher Education in the Specialty 125 "Cybersecurity" for the First (Bachelor's) Level of Higher Education") https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf

Table 3

Matrix of correspondence of program competencies to the components of the educational and professional program

List of competencies	GEN 101	GEN 109	GEN 110	GEN 120	GEN 250	GEN 300	SDT 150	SDT 151	SDT 100	SDT 101	SDT 105	SDT 107	SDT 111	SDT 112	SDT 113	SDT 202	SDT 222	SDT 223	SDT 250	SDT 252	SDT 302	SDT 303	SDT 304	SDT 305	SDT 312	SDT 314	SDT 315	SDT 316	SDT 421	SDT 423	SDT 491	SDT ???
ZK01							+	+	+	+	+	+							+	+			+			+		+			+	+
ZK02	+						+	+	+	+	+	+	+	+					+	+						+						+
ZK03			+																													+
ZK04	+																															+
ZK05	+						+	+	+	+	+	+							+	+						+	+	+				+
ZK06					+	+																										+
ZK07				+										+																		+
ZK08		+	+																+											+	+	+
SK01						+								+															+	+	+	+
SK02									+	+	+	+	+			+			+	+	+	+			+	+		+			+	+
SK03														+								+						+			+	+
SK04									+	+	+	+				+						+		+	+	+		+			+	+
SK05											+										+	+						+			+	+
SK06										+		+										+	+			+		+	+	+	+	+
SK07														+																	+	+
SK08							+	+							+	+	+	+	+	+											+	+
SK09											+																			+	+	+
SK10							+	+			+	+	+			+			+	+					+	+				+	+	+
SK11							+	+	+	+						+			+	+							+					

Table 4

Matrix of correspondence of learning outcomes and competencies determined by the educational and professional program

List of competencies	GEN 101	GEN 109	GEN 110	GEN 120	GEN 250	GEN 300	SDT 150	SDT 151	SDT 100	SDT 101	SDT 105	SDT 107	SDT 111	SDT 112	SDT 113	SDT 202	SDT 222	SDT 223	SDT 250	SDT 252	SDT 302	SDT 303	SDT 304	SDT 305	SDT 312	SDT 314	SDT 315	SDT 316	SDT 421	SDT 423	SDT 491	SDT ???
PH01	+		+																												+	+
RN02	+						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
RN03			+	+	+	+								+																	+	+
RN04	+	+			+				+	+		+					+		+							+		+			+	+
RN05		+	+		+				+	+		+				+	+		+				+			+			+		+	+
RN06		+	+		+				+	+		+														+	+	+			+	+
RN07												+			+		+	+		+												+
RN08							+	+	+	+							+		+											+		+
RN09			+		+	+								+															+		+	+
PH10									+	+		+	+				+		+						+	+		+				+
PH11														+								+											+
PH12																	+						+	+	+	+						+
PH13										+	+	+									+					+		+			+	+
PH14																					+			+				+				+
RN15													+								+				+							+
PH16																							+			+			+			+
PH17														+						+									+		+	+
PH18															+		+	+														+
PH19															+														+			+
PH20											+																			+		+
PH21													+						+						+			+			+	+
PH22									+	+						+			+	+							+					+

Structural and logical scheme of the educational and professional program