AGREED
Chairman of the Educational and Methodological Council JSC «International University of Information Technologies»
_____ A.K. Mustafina
_____ 2023

APPROVE
Rector
JSC «International University of Information Technologies»
_____ A.K. Khikmetov
_____ 2023

EDUCATIONAL PROGRAM
7M06108 «Computer technology and cybersecutity»

Education Area Code and Classification: 7M06 - Information and Communication Technologies
Code and classification: 7M061 - Information and Communication Technologies
Group of educational programs: M094- Information and Communication Technologies
Level according to the International Standard Classification of Education (ISCE): 7
Level according to National Qualifications Framework (NQF):7
Level according to Industry Qualifications Framework (IQ): 7
Duration of study: 2 years
Credits: 120

AGREED
Director of the Chairman of the ALE «Kazakhstan Information Security Association»
_____ V.V. Pokusov
_____2023

AGREED
General director of the National Innovation Center
_____
_____2023

Almaty, 2023

Table of contents

List of abbreviations and symbols

IN	Higher education
GOSO	State obligatory standard of education
ECR	European Qualifications Framework
ETF	European Education Foundation
ZUN	Knowledge, skills, skills
NKZ	National Classifier of Occupations
NRK	National Qualifications Framework
NSC	National system of qualifications
OGM	General humanitarian module
OM	General module
OP	Educational program
OPM	General professional module
ORC	Sectoral Qualifications Framework
PS	professional standard
air defense	Postgraduate education
PC	Professional competence
PM	Professional module
WG	Working group
RK	The Republic of Kazakhstan
RO	Learning Outcome
CM	Special module
QMS	Quality Management System
SAM	Socio-economic module
TVE	Technical and Vocational Education
TVET	Technical and vocational education and post-secondary education
UNESCO	United Nations Educational, Scientific and Cultural Organization/
UNESCO	specialized agency of the United Nations Educational, Scientific and Cultural Affairs.
Cedefop	European Center for the Development of Vocational Training
DACUM	from English. Developing Curriculum
ECVET	European Credit System for vocational education and training
EQAVET	European Quality Assurance in Vocational Education and Training
ENQA	EuropeanAssociationforQualityAssuranceinHigherEducation/European-Russian Association for Quality Assurance in Higher Education
ESG	Standards and Guidelines for Quality Assurance in the European Higher Education Area
FIBAA	International agency (non-profit foundation) for accreditation and examination of the quality of higher education (Bonn, Germany)
IQM-HE	Internal Quality Management in Higher Education
TACIS	Technical Assistance for the Commonwealth of Independent States
WSI	WorldSkills International

1. Description of the educational program

The educational program "Computer Technologies and Cybersecurity" is the training of highly qualified managerial personnel with in-depth professional training for various industries covering advanced computer technologies, software security, computer expertise and programming.

Computer technology and cybersecurity Specialist – an employee engaged in the design and protection of IT infrastructure and its implementation.

Specialization options include the provision of interaction and management of IoT devices, the use of artificial intelligence systems with machine learning and its implementation. with the analysis of huge amounts of information, the use of modern quantum, blockchain and cloud technologies to support and maintain the IT infrastructure of companies.

The educational program "Computer Technologies and Cybersecurity" offers theses for undergraduates who want to gain research experience in addition to mandatory electives and core courses such as management and monitoring of cybersecurity processes, legal aspects of cybersecurity and building applications using modern DevOps engineering principles.

The main activity of a computer technology and cybersecurity specialist is related to computer systems and means of processing, storing and transmitting information; information security services; mathematical models of processes that occur during information protection.

2. Purpose and objectives of the educational program

Purpose of the EP- The purpose of the educational program "Computer Technologies and cybersecurity" is to train highly qualified specialists who are able to effectively implement, analyze and ensure the security of modern computer technologies in various fields. The program is aimed at developing undergraduates' deep knowledge and practical skills in the field of computer technology, artificial intelligence, cybersecurity and related disciplines, contributing to the creation of innovative and reliable solutions for complex information tasks.

Tasks of the EP:

1. Analyze the compliance of hardware and software with the requirements of the company's internal business processes.
2. To diagnose the security of the information structure of the enterprise.
3. To support the ability to work of complex information security systems using advanced IT technologies.
4. Define the data criteria for searching and extracting data.
5. Determine additional requirements of the enterprise for IT support.
6. Develop an application architecture for iOS
7. Design and survey and research activities.

3. Requirements for evaluating the learning outcomes of an educational program

The following forms of exams are used as an assessment of learning outcomes: computer testing, written exam (answers on sheets), oral exam, project (passing a course project), practical (open questions on a computer, solving problems on a computer), complex (test / written / oral + others). In accordance with table 1, the following ratio of exam forms is recommended:

Table 1

No.	Exam form	Recommended share, %
1	Computer testing	20%
2	Writing	10%
3	Oral	5%
4	Project	30%
5	Practical	30%
6	Complex	5%

The final certification ends with the defense of the master's work.

4. Passport of the educational program

4.1 General information

No.	Field name	Note
1	Code and classification of the field of education	7M06 - Information and communication technologies
2	Code and classification of areas of study	7M061 - Information and communication technologies
3	Group of educational programs	M094 - Information and communication technologies
4	Name of the educational program	7M06108-Computer technology and Cybersecurity
5	Brief description of the educational program	The educational program "Computer Security" is to provide practice-oriented and managerial training of graduates in the field of management, creation, use and protection of information technologies designed to work in various industries and in business.
6	Purpose of the OP	The goal of the Educational Program "Computer Security" istraining of highly qualified managerial personnel with in-depth professional training for various sectors of the economy using information security systems.
7	ISCED level	7
8	NQF level	7
9	ORC level	7
10	**List of competencies of the educational program:** OK1. Develops and improves personality traits with the help of philosophy of science, psychology, pedagogy, scientific methods of research and communication in foreign languages. KK1. Control and analysis of the effectiveness of the use of software and hardware for information protection and information security, as well as system analysis and decision making KK2.Monitoring, event management and modeling of information security processes KK3. Use of blockchain and DevOps technologies, as well as the Internet of things and big data analytics KK4.Investigation of information security incidents and knowledge of legal regulations KK5. Data protection using cryptography, cryptanalysis and quantum cryptography. KK6.Administration and integration of IT processes using AI, machine learning	
11	Learning outcomes of the educational program: LO1. He has the skills to apply the methods of pedagogy and management psychology in a team, manages the processes of professional activity with management tools, and also knows how to communicate in foreign languages. LO2. He knows how to organize and apply the methods of scientific activity and uses the historically existing philosophical aspects that he applies in solving corporate problems. LO3. Conducts systematic data analysis, critically assesses the state of resources and, based on this, makes strategic decisions. Uses legal legislation and legal responsibility of objects and subjects when identifying information security incidents. LO4. He is engaged in monitoring information security processes and is able to solve issues of organizing and managing information security processes. Applies techniques for modeling information security processes.	

	LO5. Demonstrates in-depth knowledge in the investigation of information security hacker incidents using machine learning algorithms and neural networks. LO6. Conducts analysis of big data in the field of cybersecurity, knows the principles of the Internet of things technologies. Applies artificial intelligence for big data analytics. LO7. Knows the features of the use of modern encryption algorithms, knows how to apply advanced cryptanalysis methods, uses quantum cryptography and blockchain technologies in cybersecurity LO8. Uses modern solutions in the field of information security hardware. Able to integrate various IT processes. LO9. Knows the features of creating applications using DevOps.	
12	Form of study	full-time
13	Languages of instruction	English
14	Volume of loans	120
15	Awarded Academic Degree	Master in information and communication technologies in the educational program "7M06108-Computer technology and Cybersecurity "
16	Developer(s) and authors:	JSC "International University of Information Technologies", Department of Computer Engineering and Information Security: - Amanzholova S.T. assistant professor, Ph.D. - Sagymbekova A.O. senior lecturer

4.2. Matrix of correlating the learning outcomes of the educational program as a whole with the formed competencies

	LO1	LO2	LO3	LO4	LO5	LO6	LO7	LO8	LO9
OK1	V	V							
KK1			V					V	
KK2				V					
KK3						V	V		V
KK4					V				
KK5							V		
KK6								V	

4.3. Information about modules / disciplines (if there are modules, it is necessary to highlight them)

No.	Name of the discipline	Brief description of the discipline (30-50 words)	Number of credits	Formed competencies (codes)	Prerequisites	Postrequisites
Cycle of basic disciplines University component						

1	History and philosophy of science	The course is devoted to the presentation of the most important issues of the philosophy of science in connection with its development in various historical periods. The discipline is aimed at acquiring knowledge about the properties of science as a type of cognition and as a socio-cultural phenomenon in its historical development.	4	OK1	No	Writing and defending a master's thesis
2	Foreign language (professional)	Professional in-depth knowledge of the English language.	4	OK1	No	Writing and defending a master's thesis
3	High School of Pedagogy	To provide undergraduates with knowledge about the theoretical foundations of pedagogical theory and pedagogical skills, management of the educational process for teaching in higher education.	4	OK1	No	Writing and defending a master's thesis
4	Psychology of management	Management psychology is a branch of psychological science that studies the psychological patterns of management activity and sets the task of analyzing the psychological conditions that increase the efficiency and productivity of any management system.	4	OK1	No	Writing and defending a master's thesis
5	Teaching practice	Consolidation of teaching skills	4	OK1	Pedagogy of higher education, Psychology of management	Writing and defending a master's thesis
	Cycle of basic disciplines Selectable Component					
6	**Elective discipline 1**					
	Research methodology	Development of creative thinking among undergraduates in solving specific production problems, instilling skills in the search, analysis and generalization of scientific and technical information, familiarization with the basics of theoretical and experimental research.	5	OK1	History and philosophy of science Foreign language (professional)	Writing and defending a master's thesis
7	**Elective discipline 2**					

	System analysis and decision making	The fundamentals of system analysis and decision-making are considered, including the methodology and methods of system analysis, decision-making and the study of control systems for various types of activities. The use of approaches for the formation of estimates for decision-making under conditions of certainty, as well as under conditions of uncertainty.	5	KK1	No	Writing and defending a master's thesis
	Computer technology and cybersecurity process management	The course is devoted to modern best practices for organizing the work of information security services of Organizations based on the ITIL library of excellence (IT Infrastructure Library) and the international standard ISO / IEC 17799 (Information technology - information security management practices). The course allows students to gain the necessary knowledge for the effective organization and implementation of the information security process.	5	KK2	No	Writing and defending a master's thesis
8	**Elective discipline 3**					
	Modeling of Computer Technology and Cybersecurity Processes	The course is designed to study queuing models and their characteristics, as applied to real processes, and the field of IT. And modeling of information security processes	5	KK2	No	Writing and defending a master's thesis
	Monitoring of information exchange processes	The study of the information security event monitoring system (ISMS) designed to automate the process of collecting and analyzing information about security events coming from various sources. Such sources can be information security tools, general system and application software, telecommunications software, etc.				
		Major disciplines				
9	**Elective discipline 4**					
	Legal support of computer technologies and cybersecurity	Undergraduates will apply the system of legal regulation of information security of the Republic of Kazakhstan. Study the main legal acts, use significant legal actions in the field of information security. Also study information systems and electronic resources for protection, study	5	KK6	No	Writing and defending a master's thesis

		information security in state and non-state bodies. Be able to identify violations in the field of information security, such as disciplinary liability, civil liability, administrative liability and criminal offenses and crimes in the field of information security.				
10	**Elective discipline 5**					
	Quantum technology	Quantum cryptography is a branch of cryptography that uses the principles of quantum mechanics to secure communications. Unlike classical cryptography, which relies on mathematical algorithms and the complexity of data protection, quantum cryptography is based on the laws of physics, making it more secure from attacks.	5	KK5	No	Writing and defending a master's thesis
11	**Elective discipline 6**					
	Cloud resource management	The discipline is designed to study methods for distributing computing load and storage using cloud services. During the discipline, undergraduates will get acquainted with cloud platforms, master the methods of deploying disk spaces, learn how to calculate the distribution and optimization of the load on cloud servers	5	KK5	No	Writing and defending a master's thesis
	Virtualization technologies	The main goal of this discipline is the study and development of modern methods and virtualization tools. During the course, undergraduates will perform a number of tasks to deploy their own virtual space and use ready-made virtualization services to create a virtual IT infrastructure, as well as learn full and partial integration into virtual spaces.				
12	**Elective discipline 7**					
	DevOps	Undergraduates will be able to synchronize the stages of software product development, QA, and will automate their tasks, be able to program and quickly learn new tools. They will apply a methodology that helps automate workflows and make them seamless, which increases the	5	KK3	No	Writing and defending a master's thesis

		speed and productivity of developers, testers and system administrators. When developing a work plan, undergraduates will be able to determine which architecture to use in the program, how exactly the scaling will take place, which orchestration system is best to use. Further, they will be able to automate code verification, server configuration, and testing.				
	Distributed computing using blockchain	The course is dedicated to the application of blockchain technologies in distributed resources. The course also considers the practical use of blockchain technologies when creating applications, when used in conjunction with artificial intelligence technologies, for filtering and identifying, and using blockchain technologies in big data analysis.				
13	**Elective discipline 8**					
	Internet of Things and big data analytics	The basic basic principles of IoT, their ubiquitous communication infrastructure, the global identification of each object, the ability of an object to send and receive data via a personal network or the Internet are considered. The main areas of application of IoT are described. The powerful possibilities of IoT technology for the development of global science and international collaboration are shown. Examples of modern international scientific projects based on IoT technology are given. Challenges of virtually unlimited possibilities in the field of generating, collecting, transmitting, analyzing and distributing a huge amount of data on a global scale.	5	KK3	No	Writing and defending a master's thesis
	Machine learning	As a result of the training, undergraduates will apply machine learning methods at all stages of the threat detection process: from scalable clustering methods used to pre-process the stream of incoming files in the infrastructure, to reliable and compact models for behavioral analysis, which are created based on deep neural networks and work directly on user devices. They will develop these				

		technologies taking into account the serious requirements for machine learning methods to ensure information security in the real world. These requirements include: an extremely low percentage of false positives, model interpretability and resistance to the actions of a potential adversary.				
14	**Elective discipline 9**					
	Investigation of IT incidents	The course is devoted to methods of investigating hacker incidents. The sequences of numerous tests to identify the facts of a hacker's penetration into the system are described and recommendations are proposed for tracking the actions of a potential intruder.	5	KK4	No	Writing and defending a master's thesis
15	**Elective discipline 10**					
	Hardware technologies for SMART systems	Familiarization of undergraduates with modern hardware components of SMART systems, mastering methods for solving problems of creating smart devices. As a result of mastering the discipline, the ability to perform installation, configuration and maintenance of software, hardware and software and their components for various SMART systems.	5	KK6	No	Writing and defending a master's thesis
	IT process integration	As a result of training, undergraduates will apply data and process integration methods in existing IT systems, they will also use integration projects to build service-oriented and event-oriented architectures. They will be able to choose the best platforms for solving integration problems, as well as audit, analyze and optimize business processes. Solve the problem of determining the optimal-sufficient set and migration path of legacy IT systems based on the construction of ontological models, also conduct complex testing and maintenance of integration solutions.				
16	**Elective discipline 11**					

	Artificial intelligence and analytics	As a result of training, undergraduates will have the skills to manage big data, apply machine learning algorithms, pre-process data arrays, analyze data and present results. They develop AI-based solutions for various tasks and industries, conduct technical audits for the potential of implementing AI solutions, and train personnel through specialized programs.	5	KK6	No	Writing and defending a master's thesis
	Neural networks	The objectives of the course are to prepare students in the field of application of modern methods for solving problems that are difficult to formalize and require large computing power. The study of the course is aimed at preparing students to solve practical problems of data processing, mathematical modeling, informatics, obtaining a higher professional education that allows the graduate to work successfully in the chosen field of activity using modern computer technologies.				

4.4. List of modules and learning outcomes

Name of the educational program:**7M06108 "Computer technology and Cybersecurity" (Computer technology and Cybersecurity)**

Qualification: Master of information security

Module code / Module name	Module labor intensity in credits	Learning Outcomes	Criteria for evaluating learning outcomes	Disciplines forming the module Code / Name
GENERAL EDUCATIONAL MODULES				
Psychological Research Module	29	LO2, LO3, LO1	O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	History and philosophy of science
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Psychology of management
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Research Methodology
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Foreign (professional) language
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	High School of Pedagogy

			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Teaching practice
BASIC MODULES				
Security technology module	15	LO5, LO7, LO8, LO9	O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	DevOps
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Legal support of computer technologies and cybersecurity
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Cloud resource management
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Virtualization technologies
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Monitoring of information exchange processes
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Quantum technology
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F -	Distributed computing using blockchain

			the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Hardware technologies for SMART systems
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	IT process integration
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Modeling of Computer Technology and Cybersecurity Processes
PROFESSIONAL MODULES				
Forensic module	10	LO4, LO5, LO6	O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Investigation of IT incidents
Data Analysis Module	20	LO2, LO3, LO5	O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Machine learning
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Artificial intelligence and analytics
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	System analysis and decision making

			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Internet of Things and big data analytics
			O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Neural networks
Information security management module	15	LO2, LO3, LO5	O=(F/P)*100% where O - assessment of academic performance (training, productivity), F - the actual amount of acquired knowledge, skills; P - the full amount of knowledge, skills proposed for assimilation	Information security process management

5. Curriculum of the educational program

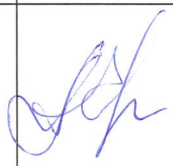
Module code	Module name	The cycle of discipline	Discipline Component	Discipline code	Name of the discipline	Academic credits	Control by academic periods				Volume in hours							Distribution of credits by academic periods			
							Exams	Differentiated test	Differentiated	Practice/R&D	Total	classroom	including			MSIWT	MSIW	1 course		2 course	
													Lectures	Practical	Lab practicals			1	2	3	4
																		Weeks in academic period			
																		15	15	15	15
1		BS	UC	SPS 7001	History and philosophy of science	4	1				45.0	30.0	1/15	1/15		1/15		4.0			
2		BS	UC	SPS7002	Pedagogy of higher education	4	1				45.0	30.0	1/15	1/15		1/15		4.0			
3		BS	UC	SPS7003	Psychology of management	4	2				45.0	30.0	1/15	1/15		1/15			4.0		
4		BS	UC	PP7201	Teaching practice	4					120.0								4.0		
5		BS	UC	LAN7001A	Foreign language (professional)	4	2				45.0	30.0		2/30		1/15			4.0		
6		BS	ES	SEC7219	Information security hardware	5	2				60.0	45.0	1/15		2/30	1/15			5.0		
7		BS	ES	SEC7210	IT process integration		2				60.0	45.0	1/15		2/30	1/15					
8		BS	ES	SEC7208	Artificial intelligence and data analytics	5	2				60.0	45.0	1/15		2/30	1/15			5.0		
9		BS	ES	SEC7207	Neural networks		2				60.0	45.0	1/15		2/30	1/15					
10		BS	ES	SEC 7212	Internet of Things and big data analytics in cybersecurity	5	3				60.0	45.0	1/15		2/30	1/15				5.0	
11		BS	ES	SEC 7213	Machine learning in information security		3				60.0	45.0	1/15		2/30	1/15					
12		AS	CS	PP7203	Research practice	8					0.0										8.0

13		AS	UC	RW7201	Research Methodology	5	1				45.0	30.0	1/15	1/15		1/15		5.0			
14		AS	UC	SEC7232	quantum cryptography	5	1				45.0	30.0	1/15		1/15	1/15		5.0			
15		AS	UC	SEC7202	Information security process management	5	2				120.0	105.0	6/90		1/15	1/15			5.0		
16		AS	UC	SEC7201	System analysis and decision making	5	3				60.0	45.0	1/15		2/30	1/15				5.0	
17		AS	UC	SEC7215	Investigation of hacker incidents	5	3				60.0	45.0	1/15		2/30	1/15				5.0	
18		AS	UC	SEC7216	Legal Liability for Information Security Incidents	5	3				60.0	45.0	1/15	2/30		1/15				5.0	
19		AS	ES	SEC 7205	Research on encryption algorithms	5	1				60.0	45.0	1/15		2/30	1/15		5.0			
20		AS	ES	SEC7206	Advanced cryptanalysis		1				60.0	45.0	1/15		2/30	1/15					
21		AS	ES	SEC 7203	Monitoring of information security processes	5	1				45.0	30.0	1/15	1/15		1/15		5.0			
22		AS	ES	SEC 7204	Modeling information security processes		1				45.0	30.0	1/15	1/15		1/15					
23		AS	ES	SEC7217	Devops	5	3				60.0	45.0	1/15		2/30	1/15				5.0	
24		AS	ES	SEC7218	Blockchain technologies in cybersecurity		3				60.0	45.0	1/15		2/30	1/15					
25		RW	CS	RW7001	Research work of a master student, including an internship and a master's thesis (NIRM)	2					0.0							2.0			
26		RW	CS	RW7002	Research work of a master student, including an internship and a master's thesis (NIRM)	3					0.0								3.0		
27		RW	CS	RW7003	Research work of a master student, including an internship and a master's thesis (NIRM)	5					0.0									5.0	
28		RW	CS	RW7008	Research work of a master student, including an internship and a master's thesis	14					0.0										14.0
Total of theoretical training						76	16	0	0	0	1380	675	300	135	240	240	0	30	30	30	22

AC	**Additional courses**	28					120.0										
TP	Teaching practice	4		2		2	120										
NIRM	Research work of a master student, including an internship and a master's thesis (NIRM)	24				1, 2, 3, 4	0										
FA	**Final attestation**	8					240.0										
	Registration and defense of a master's thesis	8				4	240										
	Total	112					1620	675	300	135	240	240	0				

6.Approval sheet with developers

Name of the educational program: 7M06108 "Computer technology and Cybersecurity"

No. p / p	Position, scientific or academic degree and Surname I.O. educational program developer	Date	Painting	Note
1	Amanzholova Saule Toksanovna Candidate of Technical Science Assistant Professor	05/21/2023		
2	Sagymbekova Azhar Oryngalievna Master of Engineering Senior Lecturer	05/21/2023		
3	Makilenov Shakirt Nurlybekovich Master of Engineering Senior Lecturer	05/21/2023		
4	Yeskendirova Damelya Maksutovna Candidate of Technical Science Assistant Professor	05/21/2023		
5	Sanim Diana Tenelkyzy Master of Engineering Lecturer	05/21/2023		