



SATBAYEV
UNIVERSITY

Institute of automation and information technologies
Department of cybersecurity, information processing and storage

EDUCATIONAL PROGRAM
7M06301 «Comprehensive information security»

Code and classification of the field of education: **7M06 «Information and communication technologies»**

Code and classification of training directions: **7M063 «Information security»**

Group of educational programs: **M095 «IT security»**

Level based on NQF: **7**

Level based on IQF: **7**

Study period: **2 years**

Amount of credits: **120**

Almaty 2023

Educational program 7M06301 «Comprehensive information security» was approved at the meeting of K.I.Satbayev KazNRTU Academic Council Minutes # 3 dated «27» October 2022.

Was reviewed and recommended for approval at the meeting of K.I.Satbayev KazNRTU Educational and Methodological Council Minutes # 2 dated «21» October 2022.

Educational program 7M06301 «Comprehensive information security» was developed by Academic committee based on direction 7M063 «Information security».



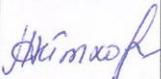


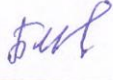
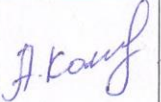


Full name	Academic degree/ academic title	Position	Workplace	Signature
Chairperson of Academic Committee:				
Viktor V. Pokusov		Chairman	Kazakhstan Information Security Association	
Teaching staff:				
Ryshan Zh. Satybaldieva	Candidate of Technical Sciences	Head of the Department "Cybersecurity, Information Processing and Storage", Associate Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 70-60	
Evgeniya Zh. Aitkhozhayeva	Candidate of Technical Sciences, docent	Associate Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Galim Z. Kaziev	Doctor of Technical Sciences	Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Dulat N. Shukaev	Doctor of Technical Sciences	Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Birzhan I. Zhumagaliev	Candidate of Technical Sciences, docent	Associate Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Employers:				
Amiret T. Konuspaev	Candidate of Physical and Mathematical Sciences	President	Association of Innovative Companies of the Special Economic Zone "Park of Innovative Technologies"	
Orken Zh. Mamyrbayev	PhD, Associate Professor	Deputy General Director	RSE "Institute of Information and Computing Technologies"	
Students				
Atkeldy Ogan		1st year doctoral student	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", mobile phone:+77076665721	

Table of contents

	List of abbreviations and designations	4
1	Description of educational program	5
2	Purpose and objectives of educational program	5
3	Requirements for the evaluation of educational program learning outcomes	6
4	Passport of educational program	7
4.1	General information	7
4.2	Relationship between the achievability of the formed learning outcomes according to educational program and academic disciplines	12
5	Curriculum of educational program	21

List of abbreviations and designations

EP – educational program
BC – basic competencies
PC – professional competencies
LO – learning outcomes
MOOC – massive open online courses
NQF – National Qualifications Framework
IQF – Industry Qualifications Framework
IS – information security

1. Description of educational program

The educational program 7M06301 "Integrated information security" is aimed at training undergraduates of the scientific and pedagogical direction. The program includes basic and specialized disciplines with the achievement of relevant competencies, as well as the passage of various types of practices (research, teaching and internships).

The professional activity of the masters is aimed at the field of information protection and security, namely, comprehensive information security and engineering and technical protection of information.

The training of masters of the scientific and pedagogical direction in information security will be carried out according to the updated educational program 7M06301 "Integrated information security". The programs of disciplines and modules of the educational program have an interdisciplinary and multidisciplinary nature, are developed taking into account the relevant educational programs of the world's leading universities and the international classifier of professional activity in the field of information security.

The educational program ensures the application of an individual approach to students, the transformation of professional competencies from professional standards and qualification standards into learning outcomes and ways to achieve them.

The educational program was developed on the basis of an analysis of the labor functions of an information security administrator, an information security auditor, and an information security engineer stated in professional standards.

The main criterion for the completion of master's degree programs is the development of all types of educational and scientific activities of a graduate student.

In case of successful completion of the full course, the student is awarded the degree of Master of Technical Sciences in the educational program 7M06301 "Integrated information security".

A graduate can perform the following types of work:

- design and engineering;
- production and technological;
- experimental research;
- organizational and managerial;
- operational;
- scientific research.

Representatives of Kazakhstani companies and associations, specialists of departmental structures in the field of protection and security participated in the development of the educational program.

2. Purpose and objectives of educational program

Purpose of EP: Provide training of specialists in scientific activities and production in the field of information security, who are able to apply various technologies, knowledge, skills and competencies in the organization, management

and design of information protection systems.

Tasks of EP:

Training of highly qualified specialists who are able to solve the following tasks:

- planning of information security audit work;
- organizational support of information security audit;
- analysis of compliance of design, operational and technical documentation on information security with the requirements in the field of ICT and IS of the object of IS audit;
- analysis of the current security status of the IS audit object;
- identification and elimination of vulnerabilities;
- monitoring and investigation of IS incidents;
- development of a model of IS threats in enterprises;
- development of technical specifications for the creation of an information security system.

The Master of the educational program 7M06301 "Integrated information security" is focused on the independent determination of the purpose of professional activity and the choice of adequate methods and means to achieve them, the implementation of scientific, innovative activities to obtain new knowledge. In addition, it is focused on the organization, design, development, management and audit of information protection and security systems for applied purposes for all sectors of the economy, government organizations and other fields of activity.

The program is designed to implement the principles of the democratic nature of education management, expand the boundaries of academic freedom and the powers of educational institutions, which will ensure the training of qualified, highly motivated personnel for innovative and knowledge-intensive sectors of the economy.

The educational program ensures the application of an individual approach to students, the transformation of professional competencies from professional standards and qualification standards into learning outcomes and ways to achieve them.

The educational program was developed on the basis of an analysis of the labor functions of an information security administrator, an information security auditor, and an information security engineer stated in professional standards.

Representatives of Kazakhstani companies and associations, specialists of departmental structures in the field of protection and security participated in the development of the educational program.

3. Requirements for evaluating the educational program learning outcomes

The educational program was developed in accordance with the State mandatory Standards of higher and Postgraduate Education, approved by the Order of the Minister of Science and Higher Education of the Republic of Kazakhstan dated July 20, 2022 No. 2 (registered in the Register of State Registration of

Regulatory Legal Acts under No. 28916) and reflects the learning outcomes on the basis of which curricula are developed (working curricula, individual curricula of students) and working curricula in disciplines (syllabuses). Mastering disciplines of at least 10% of the total volume of credits of the educational program using MOOC on the official platform [https://polytechonline.kz/cabinet/login/index.php /](https://polytechonline.kz/cabinet/login/index.php/), as well as through the study of disciplines through the international educational platform Coursera [https://www.coursera.org /](https://www.coursera.org/).

Evaluation of learning outcomes is carried out according to the developed test tasks within the educational program in accordance with the requirements of the state mandatory standard of higher and postgraduate education.

When evaluating learning outcomes, uniform conditions and equal opportunities are created for students to demonstrate their knowledge, skills and abilities.

When conducting an interim certification in an online form, online proctoring is used.

4. Passport of educational program

4.1. General information

№	Field name	Comments
1	Code and classification of the field of education	7M06 «Information and communication technologies»
2	Code and classification of training directions	7M063 «Information security»
3	Educational program group	M095 «IT security»
4	Educational program name	7M06301 «Comprehensive information security»
5	Short description of educational program	<p>The professional activities of graduates include: science, education, state and departmental structures, the economy and industry of the state, the field of healthcare.</p> <p>The objects of professional activity of graduates of master's degree programs in the educational program - "Integrated information security" are:</p> <ul style="list-style-type: none"> – public administration bodies; – information security departments and departments of departmental organizations; – information security departments, IT departments and departments of financial organizations; – information security departments, IT departments and departments of industrial enterprises; – higher educational institutions and scientific institutions; – departments and departments of information security of state organizations and commercial structures. <p>The main functions of the professional activity of undergraduates are: conducting research in the field of information security and security; audit, vulnerability analysis and investigation of incidents in information security systems; design, implementation, operation,</p>

		administration, maintenance and testing of information security systems of enterprises. Areas of professional activity, the following: – design, development, implementation and operation of information security systems; – analysis, testing and identification of system vulnerabilities; – information security audit.
6	Purpose of EP	Provide training of specialists in scientific activities and production in the field of information security, who are able to apply various technologies, knowledge, skills and competencies in the organization, management and design of information protection systems.
7	Type of EP	New EP
8	The level based on NQF	7
9	The level based on IQF	7
10	Distinctive features of EP	No
11	List of competencies of educational program	Requirements for the key competencies of graduates of the scientific and pedagogical Master's degree, must: 1) have an idea: – on the role of science and education in public life; – about current trends in the development of scientific knowledge; – on current methodological and philosophical problems of natural (social, humanitarian, economic) sciences; – about the professional competence of a high school teacher; – contradictions and socio-economic consequences of globalization processes; – on professional competence in the field of information protection and security; – about the technology of virtualization of resources and platforms; – on the intellectualization of information security tools; – about database protection technologies; – about cryptographic information protection algorithms; – about big data analysis. 2) know: – methodology of scientific knowledge; – principles and structure of the organization of scientific activity; – psychology of cognitive activity of students in the learning process; – psychological methods and means of improving the effectiveness and quality of training; – algorithms for cryptographic protection of information; – IS standards and IT security assessment criteria; – resource and platform virtualization technologies and virtualization systems from leading manufacturers; – threats and risks of virtualization systems, principles of

	<p>building hypervisors and their vulnerabilities;</p> <ul style="list-style-type: none"> – organization of IP networks, structure of IP packets and IP protocols; – internal organization of OS media; – methods and means of storing key information and encryption; – varieties and principles of authentication; – requirements for firewalls and intrusion detection systems; - database protection technologies and methods of designing secure databases; - organization of the database protection and security system; – methods and tools of active audit; – engineering and technical protection of information. <p>3) be able to:</p> <ul style="list-style-type: none"> – use the acquired knowledge for the original development and application of ideas in the context of scientific research; – critically analyze existing concepts, theories and approaches to the analysis of processes and phenomena; – integrate knowledge gained in different disciplines to solve research problems in new unfamiliar conditions; – by integrating knowledge to make judgments and make decisions based on incomplete or limited information; – apply the knowledge of pedagogy and psychology of higher education in their teaching activities; – apply interactive teaching methods; – to carry out information-analytical and information-bibliographic work with the involvement of modern information technologies; – to think creatively and creatively approach the solution of new problems and situations; – be fluent in a foreign language at a professional level, which allows conducting scientific research and teaching special disciplines in universities; – summarize the results of research and analytical work in the form of a dissertation, a scientific article, a report, an analytical note, etc.; - apply algorithms for cryptographic protection of information; - apply IS standards and conduct an IT security assessment; - apply virtualization systems from leading manufacturers; - identify threats and risks of virtualization systems; – apply methods and means of storing key information and encryption; – work with firewalls and intrusion detection systems; – apply database protection technologies and secure database design methods;
--	---

		<ul style="list-style-type: none"> – organize a database protection and security system; – apply methods and tools of active audit; – apply big data analysis tools. <p>4) have skills:</p> <ul style="list-style-type: none"> – research activities, solutions of standard scientific tasks; – implementation of educational and pedagogical activities on credit technology of training; – methods of teaching professional disciplines; – the use of modern information technologies in the educational process; – professional communication and intercultural communication; – oratory, correct and logical formalization of their thoughts in oral and written form; – organization and protection of database security; – conducting an IS audit; – application of algorithms for cryptographic protection of information; – identifying threats and countering them; – working with Big Data; – expanding and deepening the knowledge necessary for daily professional activities and continuing education in doctoral studies. <p>5) be competent:</p> <ul style="list-style-type: none"> – in the field of research methodology; – in the field of scientific and scientific-pedagogical activity in higher educational institutions; – in matters of modern educational technologies; – in the implementation of scientific projects and research in the professional field; – in the organization of IS systems; – in conducting an IS audit; – in ensuring the information security of the organization; – in ways to ensure constant updating of knowledge, expansion of professional skills and abilities.
12	Learning outcomes of educational program	<p>ON1. Have the ability to independently formulate research goals, establish a sequence for solving professional problems.</p> <p>ON2. Ability to design complex research and development work in solving professional problems. Proficiency in foreign languages at a professional level.</p> <p>ON3. Ability to design complex research and development work in solving professional problems. Proficiency in foreign languages at a professional level.</p> <p>ON4. Application of regulatory documents in the planning and organization of scientific and production work in the field of information security. Analyze current and future trends in the development of cryptographic information protection and apply them in practice.</p>

		<p>ON5. Understand the philosophical issues of science, the main historical stages of the development of science, be able to critically assess and analyze scientific and philosophical problems, understand the specifics of engineering science, possess the skills of analytical thinking, be competent in matters of psychology and pedagogy.</p> <p>ON6. To be able to organize a database protection and security system and apply database protection technologies, know modern and promising directions for the development of cryptographic information protection and apply it in practice.</p> <p>ON7. Be able to assess the security of network operating systems. Safely apply modern virtualization technologies. Know and apply the methods and tools for conducting information security audits.</p> <p>ON8. Be competent in cybercrime detection and computer forensics. Be able to use the means of recognizing and countering cyberattacks.</p> <p>ON9. Know technical means and methods of technical protection of information, be competent in the organization of engineering and technical protection of information.</p> <p>ON10. Be able to analyze big data, know methods and tools for analyzing big data. Ability to formulate problems, objectives and methods of scientific research.</p>
13	Education form	Full-time, online
14	Period of training	2 years
15	Amount of credits	120
16	Languages of instruction	Kazakh, Russian
17	Academic degree awarded	Master of Technical Sciences
18	Developer(s) and authors	R.Satybaldieva, E.Aitkhozhayeva

4.2. Relationship between the achievability of the formed learning outcomes based on educational program and academic disciplines

№	Discipline name	Short description of discipline	Amount of credits	Generated learning outcomes (codes)									
				ON1	ON2	ON3	ON4	ON5	ON6	ON7	ON8	ON9	ON10
Cycle of basic disciplines													
University component													
1	Foreign language (professional)	The course is designed for undergraduates of technical specialties to improve and develop foreign language communication skills in professional and academic fields. The course introduces students to the general principles of professional and academic intercultural oral and written communication using modern pedagogical technologies.	5			v							
2	History and philosophy of science (MOOC)	The subject of philosophy of science, dynamics of science, specifics of science, science and pre-science, antiquity and the formation of theoretical science, the main stages of the historical development of science, features of classical science, non-classical and post-non-classical science, philosophy of mathematics, physics, engineering and technology, specifics of engineering sciences, ethics of science, social and moral responsibility of a scientist and engineer.	3					v					
3	Higher school pedagogy (MOOC)	Undergraduates will master the methodological and theoretical foundations of higher school pedagogy, plan and organize the processes of teaching and upbringing, master the communicative technologies of subject-subject interaction between a teacher and a master in the educational process of a university.	3					v					
4	Psychology of management (MOOC)	The discipline studies the modern role and content of psychological aspects in managerial activity. The improvement of the psychological literacy of the student in the process of implementing professional	3					v					

		activities is considered. Self-improvement in the field of psychology and studying the composition and structure of management activities, both at the local level and abroad. The psychological feature of modern managers is considered.											
5	Pedagogical practice	It is aimed at the formation of practical skills and teaching methods. Pedagogical practice can be carried out during the period of theoretical training without interrupting the educational process. At the same time, undergraduates can be involved in conducting classes in the bachelor's degree.	6	v	v								
Cycle of basic disciplines Component of choice													
6	Algorithms of cryptographic protection of information	The modern cryptography and tasks connected to information security problems. The formal determination of the cryptosystem. Classical cryptosystems. Main objectives of crypto-analysis. Stream encryption. Cryptosystems with public key. Applications of mathematical simulation in cryptography. Merits and demerits of different systems. Euler and Fermat's theorems. Key management. System without transmission of a key. Problem of prime factorization. Problem of the discrete logarithm. Crypto-firmness problem. Systems of information security, diagram of the digital signature, authentication protocols and identifications.	5	v			v		v				
7	Security of Virtualization and Cloud Systems	In the process of studying the course, security issues of cloud technologies, sources of threats in cloud computing will be considered. Will be studied: cloud deployment models: public, private, hybrid clouds; cloud technology models; features and characteristics of cloud computing; information security standards in the field of cloud technologies and virtualization systems; means of ensuring the protection of cloud	5	v		v				v			

		computing; encryption; VPN networks; authentication; user isolation.											
8	Methods of cryptology and means of information protection	Magistracy. The modern cryptography and tasks connected to information security problems. The formal determination of a cryptosystem. The classical cryptosystems. Main objectives of crypto analysis. Stream encryption. Cryptosystems with public key. Applications of mathematical simulation in cryptography. Merits and demerits of different systems. Euler and Fermat's theorems. Key management, System without transmission of a key. Problem of prime factorization. Problem of the discrete logarithm. Crypto-firmness problem. Systems of information security, diagram of the digital signature, authentication protocols and identifications.	5				v		v			v	
9	Methods and means of protection in Operating systems	The course examines protection against alteration and control of the integrity of software. Methods and means of storing key information. Principles of multi-factor authentication. Identification and authentication technical devices. Encryption software and hardware. Ensuring security in Windows, Unix systems, familiarization with the internal organization of storage media. Intrusion detection systems. The main components of the firewall architecture. Modern requirements for firewalls.	5				v					v	
10	Means of security of network of operating systems	Information security bases of support of network OS. Protection against change and monitoring of integrity of the software. Methods and means of storage key information. Principles of multifactor authentication. Technical devices of identification and authentication. Password subsystems of identification and authentication. Identification and authentication of users by means of biometrics devices. Encoding software and hardware tools. Safety of network	5		v					v			

		operating systems. Safety in the systems Windows, Unix. Systems of detection of invasions. Principal components of architecture of firewalls. The modern requirements to firewalls.											
11	Scientific Python	The course studies the general principles of working with data: loading, receiving and processing unstructured data, obtaining data through the API, visualizing and publishing data, filtering, transforming, analyzing and interpreting data using well-known models of classification, clustering, regression, etc. The range of tasks covers methods optimization, stochastic modeling, Gaussian modeling, partial differential equations, Navier-Stokes equation, heat equations.	5	v	v								
Cycle of profile disciplines University component													
12	Organization of protection and safety of a database	Aspects and criteria of security, security policy. Data security threats. Database protection and security, data integrity and reliability. Methods and means of protection and data protection. Develop a secure database. CASE design tools. Database administration tools. Impressions as tools to improve data security. Effect of cursors on database security. Transaction management. stored procedures. triggers. Mandatory and discretionary access control to the DBMS. Role and reports. Monitoring and audit of DBMS. Cryptographic tools for database protection. Replication and data recovery. High training tools.	5	v					v				v
13	Organization of information security systems	The concept of information security systems. Information security systems standards. Select an object to organize the system. Threat analysis and security software development. Administrative and procedural levels of information security. Analysis and selection of information security methods.	5		v	v	v						

		Provision and evaluation of objects											
14	Research practice	The research practice of the undergraduate is conducted in order to familiarize himself with the latest theoretical, methodological and technological achievements of domestic and foreign science, modern methods of scientific research, processing and interpretation of experimental data.	8		v	v							
Cycle of profile disciplines Component of choice													
15	Data analysis and Data retrieval	The discipline is aimed to teach information retrieval and data mining techniques. It is about how to find relevant information and subsequently extract meaningful patterns out of it. While the basic theories and mathematical models of information retrieval and data mining are covered, the discipline is primarily focused on practical algorithms of textual document indexing, relevance ranking, web usage mining, text analytics, as well as their performance evaluations. Practical retrieval and data mining applications such as web search engines, personalisation and recommender systems, business intelligence, and fraud detection will also be covered.	5						v				v
16	Information Security Audit	Audit of information security. Basic terms, definitions, concepts and principles in the field of information security audit. The main directions of the audit of information security. Types and objectives of the audit. The main stages of the security audit. A list of the initial data required to conduct a security audit. Assessment of the current state of the information security system. Assessment of the level of safety. Risk analysis, assessment of the level of security, development of security policies and other organizational and administrative documents for the protection of information. Effective programs to build	5			v				v			

		an organization's security system											
17	Technical protection of information	Magistracy. Technical Protection (TP) of information. Actions for information security using passive and active technical means. Information ITZ technical means, classification. Physical security features of objects. Hardware of search and detection of channels of information leakage. Technical channels of leakage of acoustic information. Technical means of reception and information transfer. Mortgage devices of interception of the voice information. Telephone ear. Electronic stethoscopes. Laser microphones. Optical-electronic interception of audible tones by laser probing of windowpanes. The technical channel of information leakage by "high-frequency imposing". The parametric technical channels of information leakage.	5	v							v	v	
18	Intellectualized recognition and countermeasures for cyber attacks	Models, targets, tools of cyber attacks. Active protection as a method of countering advanced cyber threats. Effective counteraction. Components of active protection. Preventive network research. Analysis of anomalies. Advantages of active protection	5		v		v				v		
19	Artificial intelligence	The goal of artificial intelligence is to create technical systems capable of solving non-computational problems and performing actions that require the processing of meaningful information and are considered the prerogative of the human brain.	5		v								v
20	Cybercrime and computer forensics	The course is aimed at the study of digital evidence, methods of searching, obtaining and fixing such evidence, as well as the analysis and investigation of events in which computer information or a computer as a tool for committing a crime or other digital evidence appears. The course explores typical models of cybercriminals and their behavior, the main types of cyberattacks, as well as methods for responding,	5								v		

		investigating and documenting cyber incidents.											
21	Natural Language Processing	The course studies the theoretical and practical foundations of natural language processing. The course covers the theoretical aspects of NLP, including basic information from the field of linguistics, and practical methods of word processing. Classical text information processing algorithms are considered, such as regular expressions, measuring distances, substitutions, searching for strings and substrings. linguistic trees. Corpus of text. Taxonomy. Models Word2Vec, Text Embedding, LSTM models of neural networks are considered. Existing libraries for text information analysis are being studied.	5		v								v
22	Risk management in cyber security	The program of the training course "Risk Management in Cybersecurity" is aimed at studying international and national standards for risk management in cybersecurity, methods for determining and managing risks, the practical application of standards and methods, studying specialized software systems for risk assessment.	5							v		v	
23	Steganographic methods of information protection	The content of the discipline covers a range of issues related to the protection of information through mathematical transformations using steganographic algorithms and copyright protection algorithms.	5		v							v	
24	Technologies of protection of wireless networks (applications)	Security technology for wireless networks and mobile applications. Unified solutions. Classification of applications for mobile devices. Methods for scanning and testing mobile applications. Integrated security system for wireless networks. Analysis of the security of mobile applications. Analysis of the security of wireless networks and mobile applications. Security protocols of wireless networks. WEP encryption mechanism. Passive and active network attacks.	5		v					v	v		

		Authentication in wireless networks and mobile applications. Integrity and confidentiality of transmitted data. Deploying wireless virtual networks. Tunneling. IPSec protocol. Intrusion detection systems in wireless networks and mobile applications, their characteristics.											
25	Big Data and Data Analysis	The purpose of the course is to form students' professional competence in the development and use of systems for processing and analyzing large amounts of data. The content of the discipline examines the methods of analysis and storage of large amounts of data, the stages of the life cycle of big data processing, the languages best suited for processing and analytics of big data, ways of organizing storage and access to big data.	5			v			v				
26	Machine Learning & Deep Learning	The course focuses on deep learning models. As a field within machine learning, deep learning models exemplify the quantitative-qualitative transition. New models and their properties require a separate study and practice of setting the metaparameters of such models. This course covers deep learning fundamentals, neural networks, convolutional networks, RNN, LSTM, Adam, Dropout, BatchNorm, Xavier/He initializations.	5			v			v				v
27	OLAP and Data Warehousing	The purpose of mastering the discipline is to obtain in-depth knowledge of data storage systems and data mining and data processing technologies. The content of the discipline includes questions on the types of data models, the concept and architecture of data warehouses, the implementation of procedures and examples of modern corporate systems using OLAP technology. Upon completion of the course, undergraduates will be able to design data warehouses and apply data processing technologies to solve	5						v				v

		research problems.												
28	Security Internet of things	The purpose of mastering the course is to study the main areas of activity to ensure the security of the Internet of things, cyber-physical systems as part of critical information infrastructure facilities. As a result of mastering the discipline, undergraduates will learn to use the principles of a systematic approach; ways of forming requirements for the cybersecurity of the Internet of Things systems; the main provisions of the standards for the functional safety of process control systems ("Industrial Internet of things"); requirements of regulatory legal acts and standards for the development of information security threat models.	5	v	v									
Research work of a master's student														
29	Research work of a master's student, including internship and completion of a master's thesis	Systematization of theoretical knowledge, development of skills in setting tasks on the topic of research and their consistent solution. The research work includes an assessment of the objects of research, describing its problems, the allocation of a narrow area for research, conducting an experiment, analyzing the results of the experimental part, preparing and defending a research report and summarizing the results.	24	v	v	v								

5. Curriculum of educational program



NON-PROFIT JOINT STOCK COMPANY
«KAZAKH NATIONAL RESEARCH TECHNICAL UNIVERSITY NAMED AFTER K.I.SATBAYEV»



CURRICULUM
of Educational Program on enrollment for 2023-2024 academic year
Educational program 7M06301 "Comprehensive information security"
Group of educational programs M095 "IT Security"

Form of study: full-time Duration of training: 2 years Academic degree: master of Technical Sciences

Discipline code	Name of disciplines	Cycle	Total amount in credits	Total hours	Classroom amount lek/lab/pr	SIS (including TSIS) in hours	Form of control	Distribution of classroom classes by courses and semesters			
								1 course		2 course	
								1 semester	2 semester	3 semester	4 semester
CYCLE OF BASIC DISCIPLINES (BD)											
M-1. Module of basic training (university component and component of choice)											
LNG210	Foreign language (professional)	BD, UC	5	150	0/0/3	105	E	5			
HUM214	Psychology of management	BD, UC	3	90	1/0/1	60	E	3			
HUM212	History and philosophy of science	BD, UC	3	90	1/0/1	60	E		3		
HUM213	Higher school pedagogy	BD, UC	3	90	1/0/1	60	E		3		
SEC221	Means of security of network of operating systems	BD, CCH	5	150	1/0/2	105	E	5			
SEC211	Methods and means of protection in Operating systems				1/0/2						
CSE738	Scientific Python	BD, CCH	5	150	1/0/2	105	E	5			
SEC244	Security of Virtualization and Cloud Systems				2/0/1						
SEC201	Algorithms of cryptographic protection of information	BD, CCH	5	150	2/0/1	105	E		5		
SEC210	Methods of cryptology and means of information protection				2/0/1						
CYCLE OF PROFILE DISCIPLINES (PD)											
M-2. Module of professional activity (university component and component of choice)											
SEC215	Organization of information security systems	PD, UC	5	150	1/1/1	105	E	5			
SEC214	Organization of protection and safety of a database	PD, UC	5	150	2/0/1	105	E		5		
CSE777	Artificial intelligence	PD, CCH	5	150	2/0/1	105	E		5		
CSE283	Natural Language Processing				2/0/1						
CSE718	Technical protection of information	PD, CCH	5	150	1/0/2	105	E		5		
SEC238	Steganographic methods of information protection				1/0/2						
SEC246	Big Data and Data Analysis	PD, CCH	5	150	2/1/0	105	E			5	
CSE746	Machine Learning & Deep Learning				2/0/1						
SEC240	Cybercrime and computer forensics	PD, CCH	5	150	2/0/1	105	E			5	
SEC247	Intellectualized recognition and countermeasures for cyber attacks				2/0/1						
SEC204	Information Security Audit	PD, CCH	5	150	2/0/1	105	E			5	
SEC245	Risk management in cyber security				2/0/1						
SEC234	OLAP and Data Warehousing	PD, CCH	5	150	1/1/1	105	E			5	
CSE258	Data analysis and Data retrieval				1/1/1						
SEC248	Security Internet of things	PD, CCH	5	150	1/0/2	105	E			5	
SEC222	Technologies of protection of wireless				1/0/2						
M-3. Practice-oriented module											
AAP229	Pedagogical practice	BD, UC	6						6		
AAP269	Research practice	PD, UC	8								8
M-4. Research module											
AAP251	Research work of a master's student, including internship and completion of a master's thesis	RWMS	2					2			
AAP241	Research work of a master's student, including internship and completion of a master's thesis	RWMS	3						3		
AAP254	Research work of a master's student, including internship and completion of a master's thesis	RWMS	5							5	
AAP255	Research work of a master's student, including internship and completion of a master's thesis	RWMS	14								14
M-5. Module of final attestation											

NON-PROFIT JOINT STOCK COMPANY
«KAZAKH NATIONAL RESEARCH TECHNICAL UNIVERSITY named after K.I.SATBAYEV»

ECA213	Preparation and defense of a master's thesis	PDMT	8							8	
Total by UNIVERSITY:								25	35	30	30
								60		60	

Number of credits for the entire period of study				
Cycle code	Cycles of disciplines	Credits		
		university component (UC)	component of choice (CCh)	Total
BD	Cycle of basic disciplines	20	15	35
PD	Cycle of profile disciplines	18	35	53
	Total for theoretical training:	38	50	88
RWMS	Research work of a master's student	24		24
PDMT	Preparation and defense of a master's thesis	8		8
	Total:	70	50	120

Decision of the Academic Council of Kazntu named after K.Satpayev. Protocol № 3 "27" october 2022 y.

Decision of the Educational and Methodological Council of Kazntu named after K.Satpayev. Protocol № 2 "21" october 2022 y.

Decision of the Academic Council of the Institute Automation and Information Technologies
Protocol № 2 "21" september 2022 y.

Governing Board member - Vice-Rector for Academic Affairs

Institute Director Automation and Information Technology

Department Head "Cybersecurity, information processing and storage"

Representative of the Council from employers

 B.A. Zhautikov
 R.K. Uskenbayeva
 R.Zh. Satybaldieva
 V.V. Pokusov