Non-profit joint-stock company «KAZAKH NATIONAL RESEARCH TECHNICAL UNIVERSITY
named after K.I.Satbayev»

Institute of Technical Automation and Information TechnologiesКафедра "Cybersecurity, information processing and storage"

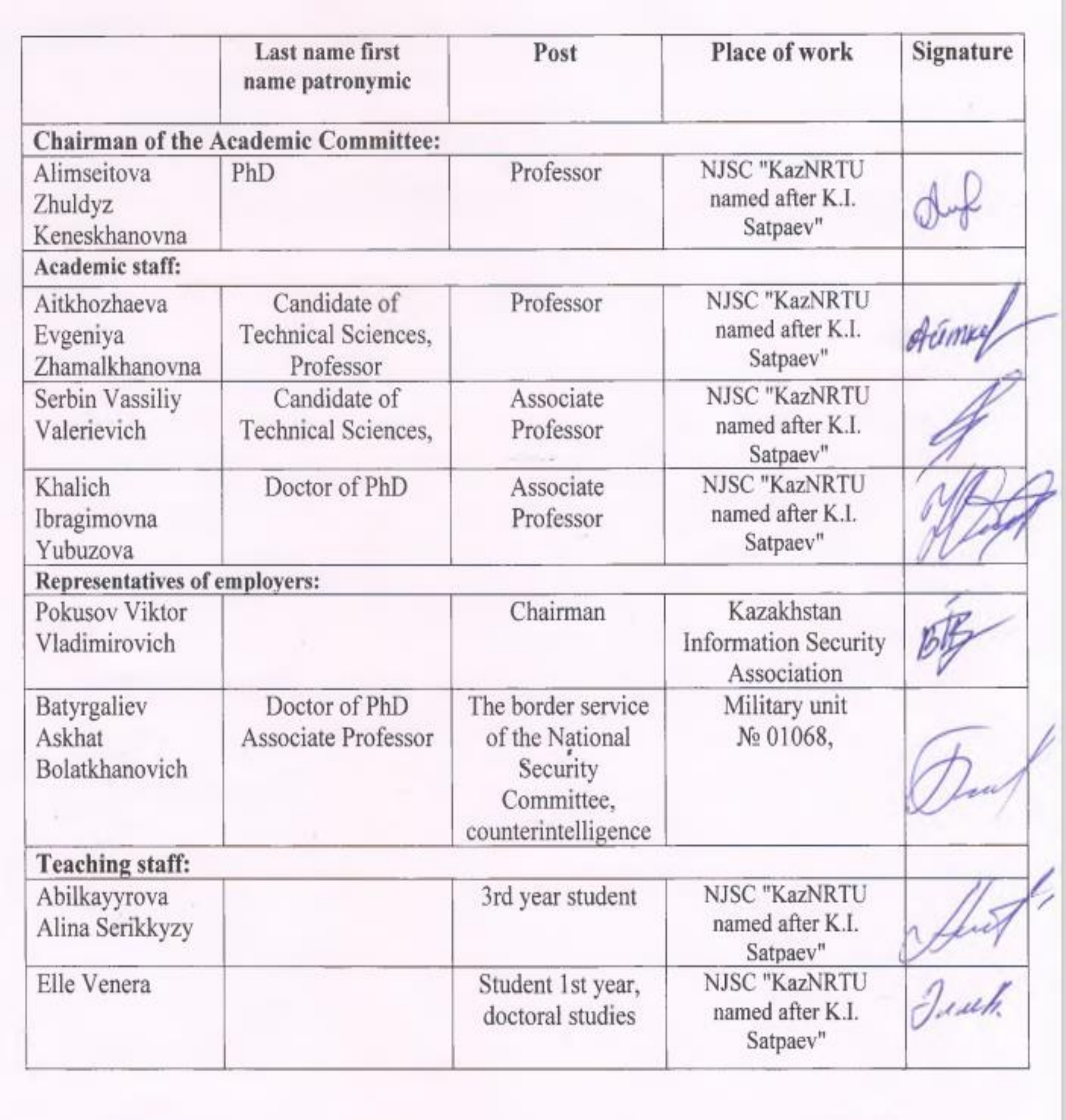
EDUCATIONAL PROGRAM
"7M06302 - Integrated information security"

Code and classification of the field of education: 7M06 Information and communication technologies
Code and classification of training areas: 7M063 Information Security
Group of educational programs: M095 Information Security
NRK Level: 7
ORC Level: 7
Duration of study: 1,5 years
Volume of credits: 90 credits

Almaty, 2025

The educational program "7M06302 - Integrated information security" was approved
at a meeting of the Academic Council of KazNTU named after K.I.Satpayev.
Protocol No. №10 of "_06___" __03__ 2025
Reviewed and recommended for approval at a meeting of the Educational and Methodological Council of Kazntu named after K.I.Satpayev.
Protocol No. №3 of "_20___" __12__ 2024

The educational program "7M06302 - Integrated information security" was developed by the academic committee in the direction "7M063 Information security"



	Last name first name patronymic	Post	Place of work	Signature
Chairman of the Academic Committee:				
Alimseitova Zhuldyz Keneskhanovna	PhD	Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Academic staff:				
Aitkhozhaeva Evgeniya Zhamalkhanovna	Candidate of Technical Sciences, Professor	Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Serbin Vassiliy Valerievich	Candidate of Technical Sciences,	Associate Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Khalich Ibragimovna Yubuzova	Doctor of PhD	Associate Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Representatives of employers:				
Pokusov Viktor Vladimirovich		Chairman	Kazakhstan Information Security Association	
Batyrgaliev Askhat Bolatkhanovich	Doctor of PhD Associate Professor	The border service of the National Security Committee, counterintelligence	Military unit № 01068,	
Teaching staff:				
Abilkayyrova Alina Serikkyzy		3rd year student	NJSC "KazNRTU named after K.I. Satpaev"	
Elle Venera		Student 1st year, doctoral studies	NJSC "KazNRTU named after K.I. Satpaev"	

Oglavlanie

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
ICT – Information and communication technologies
IT – information Technology

1. Description of the educational program

The educational program 7M06302 “Comprehensive information security” is aimed at training master’s students in a specialized field. The program includes basic and specialized disciplines with the achievement of relevant competencies, as well as various types of internships (production practice, experimental research and internship).

The professional activities of masters are aimed at the field of information protection and security, namely the comprehensive provision of information security and engineering and technical protection of information. Training of specialized masters in information security will be carried out according to the updated educational program 7M06302 “Comprehensive information security”.

The programs of disciplines and modules of the educational program are interdisciplinary and multidisciplinary in nature, developed taking into account the relevant educational programs of the world's leading universities and the international classifier of professional activities 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 based on an analysis of the labor functions of an information security administrator, information security auditor, and information security engineer, as stated in professional standards.

The main criterion for completing studies in master's programs is the mastery of all types of educational and professional activities of the master's student. Upon successful completion of the full course, the student is awarded a Master of Engineering and Technology degree in the educational program 7M06302 “Comprehensive information security.”

A graduate can perform the following types of work:

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

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

2. The purpose and objectives of the educational program

Purpose of the OP: Training of specialists for professional activities 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 security system.

OP tasks:

Training of highly qualified specialists who can solve the - planning of information security audit work following tasks:

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

The master's degree in educational program 7M06302 "Comprehensive information security" is focused on independently determining the goals of professional activity and choosing adequate methods and means to achieve them, carrying out innovative activities to obtain new knowledge. In addition, it is focused on the organization, design, development, management and audit of applied information protection and security systems for all sectors of the economy, government organizations and other areas of activit.

3. Requirements for the evaluation of learning outcomes of the educational program

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/, as well as through the study of disciplines through the international educational platform Coursera 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 the educational program

4.1. General information

№	Field name	Note
1	Code and classification of the field of education	7M06 Information and Communication Technologies
2	Code and classification of training areas	7M063 Information security
3	Group of educational programs	M095 Information security
4	Name of the educational program	7M06302 - Integrated information security
5	Brief description of the educational program	Professional activities of graduates include: education, government and departmental structures, economics and industry of the state, and healthcare. The objects of professional activity of graduates of master's programs in the educational program 7M06302 “Comprehensive information security” are: − government 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; − departments and departments of information security of government organizations and commercial structures. The main functions of the professional activities of undergraduates are: conducting research in the field of information protection and security; audit, vulnerability analysis and incident investigation in information security systems; design, implementation, operation, administration, maintenance and testing of enterprise information security systems. Areas of professional activity are the following: − design, development, implementation and operation of information security systems; − analysis, testing and identification of system vulnerabilities; − information security audit
6	The purpose of the Educational program	Training of specialists for professional activities 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 security systems
7	Type of educational program	New EP
8	The level of the NRK	7
9	ORC Level	7
10	Distinctive features of the Educational program	No
11	List of competencies of the educational program:	A graduate of a specialized master's program must: 1) have an idea:

		– about the contradictions and socio-economic consequences of globalization processes; – about 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 means; - about database protection technologies; – about algorithms for cryptographic information protection; - about big data analysis. 2) know: – psychological methods and means of increasing the effectiveness and quality of training; – algorithms for cryptographic information protection; – IS standards and IT security assessment criteria; - technologies for virtualization of resources and platforms and virtualization systems from leading manufacturers; - threats and risks of virtualization systems, principles of constructing hypervisors and their vulnerabilities; – organization of IP networks, structure of IP packets and IP protocols; – internal organization of OS storage media; – methods and means of storing key information and encryption; - types and principles of authentication; – requirements for firewalls and intrusion detection systems; - database protection technologies and methods for designing secure databases; - organization of the database protection and security system; – active audit methods and tools; – engineering and technical protection of information. 3) be able to: - critically analyze existing concepts, theories and approaches to the analysis of processes and phenomena; - integrate knowledge gained within different disciplines to solve research problems in new unfamiliar conditions; – through the integration of knowledge, make judgments and make decisions based on incomplete or limited information; – carry out information-analytical and informationbibliographic work using modern information technologies; - think creatively and have a creative approach to solving new problems and situations; – be fluent in a foreign language at a professional

		level, allowing you to conduct research; – summarize the results of analytical work in the form of a dissertation, article, report, analytical note, etc. – apply cryptographic information protection algorithms; - apply information security standards and conduct IT security assessments; - use 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 methods for designing secure databases; – organize a database protection and security system; – apply active audit methods and tools; - apply big data analysis tools. 4) have the skills: – professional communication and intercultural communication; – organization and protection of database security; – conducting an information security audit; – application of cryptographic information protection algorithms; – identifying threats and countering them; – working with Big Data; – expanding and deepening the knowledge necessary for everyday professional activities. 5) be competent: – in the organization of information security systems; – conducting an information security 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 the educational program:	**ON1.** Be able to organize a stable database protection and security system. Apply database protection technologies and secure database design methods. **ON2**. Know and apply virtualization technologies for resources and platforms and virtualization systems from leading manufacturers. Know the threats and risks of virtualization systems, the principles of building hypervisors and their vulnerabilities. **ON3.** Know the organization of IP networks, the structure of IP packets and IP protocols, the types and principles of authentication. Be able to assess the security of network operating systems **ON4.** Be competent in cybercrime detection and computer forensics. Be able to use tools for recognizing and countering cyber attacks. Know the technical means and methods of technical protection

		of information, be competent in the organization of engineering and technical protection of information. **ON5**. Be able to use regulatory documents in practice when planning and organizing scientific and production work in the field of information security. Know modern and promising areas of development of cryptographic information protection and apply it in practice. **ON6.** Be able to independently acquire, comprehend, structure and use new knowledge and skills in their professional activities, develop their innovative abilities to create an integrated stable protected infrastructure of organizations. **ON7.** Be able to analyze big data, know the methods and tools of big data analysis. The ability to formulate problems, tasks and methods of scientific research **ON8.** Be able to apply various decision support methods, promptly monitor the execution of work, resolve contradictions between team members, and manage risks arising from project implementation. Know modern standards in the field of project management and their characteristics. Proficiency in foreign languages at a professional level for partnership for sustainable development
13	Form of training	full – time. online
14	Duration of training	1.5 years
15	Volume of loans	90 credits
16	Languages of instruction	Kazakh, Russian, English
17	Academic degree awarded	Master of Technical Sciences
18	Developer(s) and authors:	Aitkhozhaeva E.Zh., Satybaldieva R.Zh.,

4.2. The relationship between the achievability of the formed learning outcomes according to the educational program and academic disciplines

№	Name of the discipline	Brief description of the discipline	Number of credits	Generated learning outcomes (codes)							
				ON1	ON2	ON3	ON4	ON5	ON1	ON7	ON8
1	Foreign language (professional)	The course is designed for undergraduates of technical specialties to improve and develop foreign language communication skills in the 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 (round table, debates, discussions, analysis of professionally oriented cases, design). The course ends with a final exam. Undergraduates also need to study independently (MIS).	2								v
2	Management	The purpose of the discipline is to form a scientific understanding of management as a type of professional activity; to master the general theoretical principles of managing socio-economic systems; to master the skills and practical solutions to management problems; to study the world experience of management, as well as the specifics of Kazakhstani management, and to teach students how to solve practical issues related to managing various aspects of organizations.	2						v		v
3	Psychology of management	The course is aimed at mastering the tools of effective employee management, based on knowledge of the psychological mechanisms of the manager's activity. The discipline will help you master the skills of decision-making, creating a favorable psychological climate, motivating employees, setting goals,	2						v		v

		building a team, and communicating with employees. At the end of the course, undergraduates will learn how to resolve managerial conflicts, create their own image, analyze situations in the field of management, as well as conduct negotiations, be stress-resistant and effective leaders.									
The cycle of basic disciplines **Component of choice**											
4	Cryptographic information protection algorithms	Modern problems of cryptography and information security. The official link to the cryptosystem. Classical cryptosystems. The main tasks of cryptanalysis. Streaming encryption. Public-key cryptosystems. The use of mathematical modeling in cryptography. Advantages and disadvantages of different systems. The theorems of Euler and Fermat. Key management. A system that doesn't have a keypad switch. Classification problems by prime factors. Problems with the discrete logarithm. Problems with cryptography. Information security systems, electronic signature schemes, authentication and authentication protocols.	5	**v**			**v**				
5	Security of virtualization and cloud technology systems	The purpose of mastering the discipline is to study the security issues of cloud technologies, sources of threats in cloud computing. The course is aimed at studying 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, cloud computing security tools, encryption, VPN networks, authentication, user isolation.	5					**v**	**v**		

6	Cryptographic methods and information security tools	Magistracy. Modern cryptography and tasks related to information security issues. The formal definition of a cryptosystem. Classical cryptosystems. The main tasks of cryptanalysis. Stream-based encryption. Public-key cryptosystems. Applications of mathematical modeling in cryptography. Advantages and disadvantages of various systems. The theorems of Euler and Fermat. Key management, a system without key transfer. The problem of prime factorization. The problem of discrete logarithmization. The problem of cryptographic security. Information security systems, electronic signature schemes, authentication and identification protocols.	5	v			v				
7	Python for solving information security problems	The course is aimed at studying the issues of solving high-level mathematical and technical problems using the NumPy and SciPy packages, and data analysis using the Pandas package. Promotes the development of skills in working with information security-related data: loading, filtering, transformation, analysis and interpretation of data using well-known models of classification, clustering, regression, etc. The basic methods of working with matrices and matrix operations are studied. Data visualization tools are being explored	5				v			v	
The cycle of profile disciplines **The university component**											
8	Organization of database protection and security	Security aspects and criteria, security policy. Threats to data security. Database protection and security, data integrity and reliability. Methods and means of data protection and protection. Develop a secure database. CASE-design tools. Database administration	5	v						v	

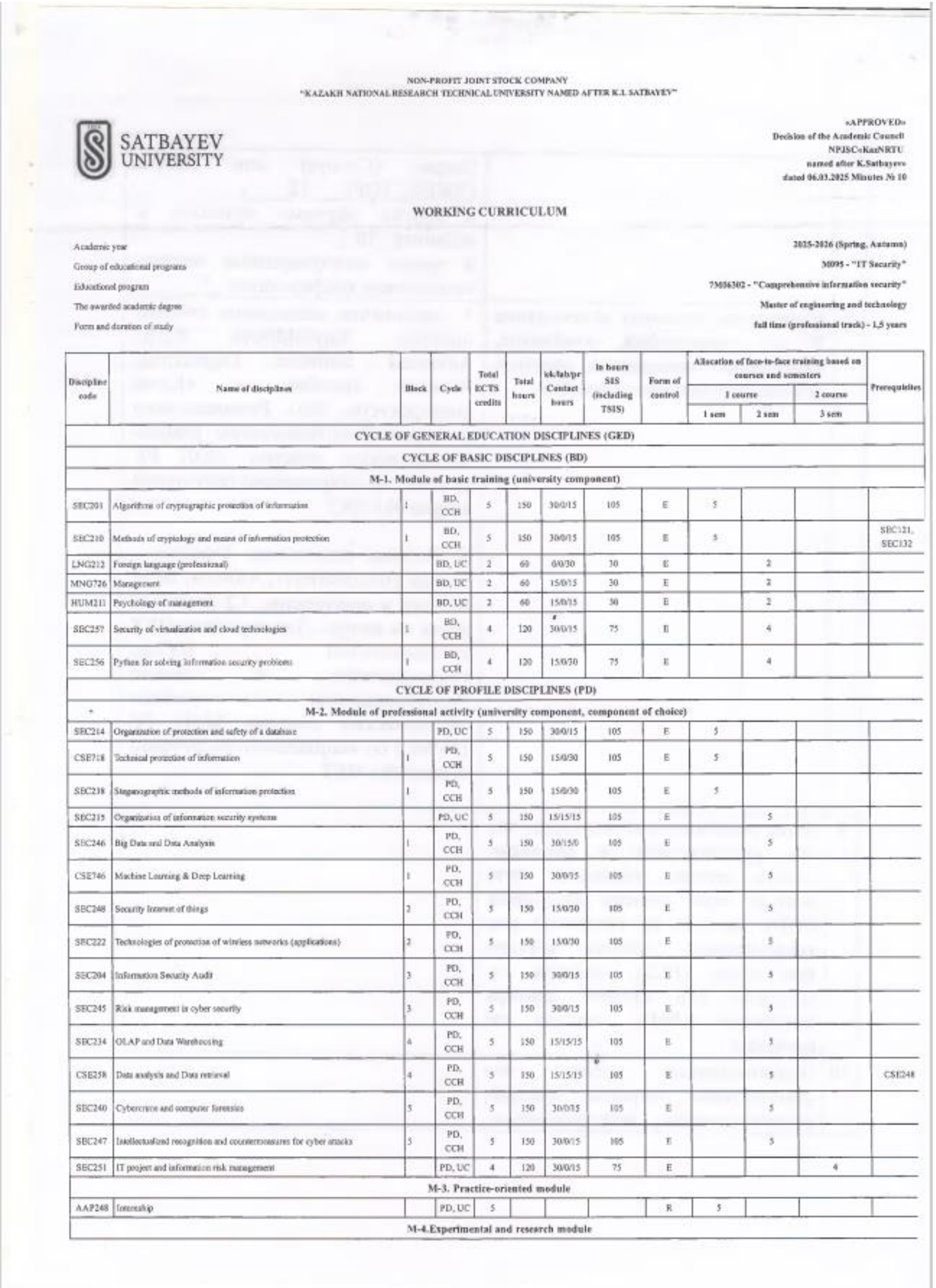
		tools. Impressions as tools for improving data security. The impact of cursors on database security. Transaction management. Stored procedures. Triggers. Mandatory and discretionary DBMS access management. Role and reports. DBMS monitoring and auditing. Cryptographic tools for database protection. Data replication and recovery. Highly trained tools.									
9	Organization of information security systems	The concept of information security systems. Standards of information security systems. 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. Provision and evaluation of facilities	5	**v**		**v**					**v**
10	Management of IT projects and information technologies рисками	The purpose of mastering the discipline is to form knowledge, skills and abilities in the field of risk management of IT projects, theoretical and practical mastery of modern risk analysis and assessment tools, study the requirements for the development of documentation on risk identification and assessment, familiarization with the principles and methods of risk management to improve business processes and IT infrastructure of the enterprise.	5			**v**			**v**		**v**
The cycle of profile disciplines **Component of choice**											
11	Data analysis and data extraction	This discipline focuses on the study of information retrieval and data mining techniques. It's about how to find relevant information and subsequently extract meaningful patterns from it. While the basic theories and mathematical models of information retrieval and data mining are	5	**v**						v	

		covered, the discipline is primarily focused on practical algorithms for indexing a text document, relevance rating, using web resources, text analytics, and evaluating their performance. Practical search and intelligent applications such as web search engines, personalization and recommendation systems, business intelligence, and fraud detection will also be covered..									
12	Information Security audit	Information Security audit Information security management. Information security audit. Basic terms, definitions, concepts and principles in the field of information security audit. The main areas of information security audit. Types and objectives of the audit. The main stages of the security audit. A list of the source data required for conducting a security audit. Assessment of the current state of the information security system. Assessment of the security level. Risk analysis, assessment of the security level, development of security policies and other organizational and administrative documents for information protection. International standards and best practices for conducting OTT audits.	5		**v**		**v**	**v**			
13	Engineering and technical information protection	Engineering Information (FROM) Information. Carrying out necessary actions to protect information using active and passive technical means. Technical means of information protection, their classification. Physical means of protecting objects. Suitable tools for searching and finding information flows. Methods of streaming audio information. Technical means for obtaining and distributing information. Unauthorized audio information device.	5	**v**	**v**						

		Headphones for your phone. An electronic stethoscope. Optoelectronic interception of sound signals using laser sensing of window panes. A technical channel for information leakage through "high-frequency overlay". Parametric technical channels of information leakage.									
14	Intelligent tools for recognizing and countering cyber attacks	Models, goals, and means of cyberattack. Active protection is a method of preventing cybersecurity. Effective counteraction. Active protection components. Network prevention. Anomaly analysis, advantages of active protection.	5					v	v		
15	Cybercrime and computer forensics	The course is aimed at the study of digital evidence, methods of searching, obtaining and consolidating such evidence, as well as the analysis and investigation of events involving computer information or a computer as a tool for committing a crime or other digital evidence. The course examines typical patterns of cybercriminals and their behavior, the main types of cyber attacks, as well as methods for responding, investigating, and documenting cyber incidents.	5		v		v		v		
16	Risk management in cybersecurity	Risk management in cybersecurity The program of the training course "Risk Management in Cybersecurity" is aimed at studying international and national standards of risk management in cybersecurity, methods of risk identification and management, practical application of standards and methods, and the study of specialized software packages for risk assessment.	5				v				v
17	Steganographic methods of information protection	The content of the discipline covers a range of issues related to the protection of	5	v			v	v			

		information through mathematical transformations using steganographic algorithms and copyright protection algorithms.									
18	Wireless network protection technologies	Security technology for wireless networks and mobile applications. Unified solutions. Classification of applications for mobile devices. Methods of scanning and testing mobile applications. Comprehensive wireless network security system. Analysis of the security of mobile applications. Threats and security risks of wireless networks and mobile applications. Wireless network security protocols. The WEP encryption mechanism. Passive and active network attacks. Authentication in wireless networks and mobile applications. Technologies for the integrity and confidentiality of transmitted data. Deployment of wireless virtual networks. Tunneling. IPsec protocol. Intrusion detection systems in wireless networks and mobile applications, their characteristics.	5			**v**		**v**	**v**		
19	Big Data and data analysis	The purpose of the course is to develop 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 analyzing and storing large amounts of data, the stages of the life cycle of big data processing, the languages most suitable for processing and analyzing big data, and ways to organize storage and access to big data.	5	**v**						**v**	
20	Machine Learning & Deep Learning	The course focuses on deep learning models. As an area within machine learning, deep learning models illustrate the quantitative-	5	**v**					**v**	**v**	

		qualitative transition. New models and their properties require separate study and practice of adjusting the meta-parameters of such models. This course covers the basics of deep learning, neural networks, convolutional networks, RN, LSTM, Adam, Dropout, BatchNorm, and Xavier/Hernandez initialization.									
21	OLAP and data warehouses	The purpose of mastering the discipline is to gain in-depth knowledge about data storage systems and data mining and processing technologies. The content of the discipline includes questions on types of data models, concepts and architecture of data warehouses, 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 research problems.	5							v	v
22	Security Internet of things	The purpose of the course is to study the main areas of activity for ensuring 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 how to use the principles of a systematic approach; ways to form requirements for cybersecurity of Internet of Things systems; the main provisions of standards for the functional security of automated control systems ("Industrial Internet of Things"); requirements of regulatory legal acts and standards for the development of information security threat models.	5			v	v				



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

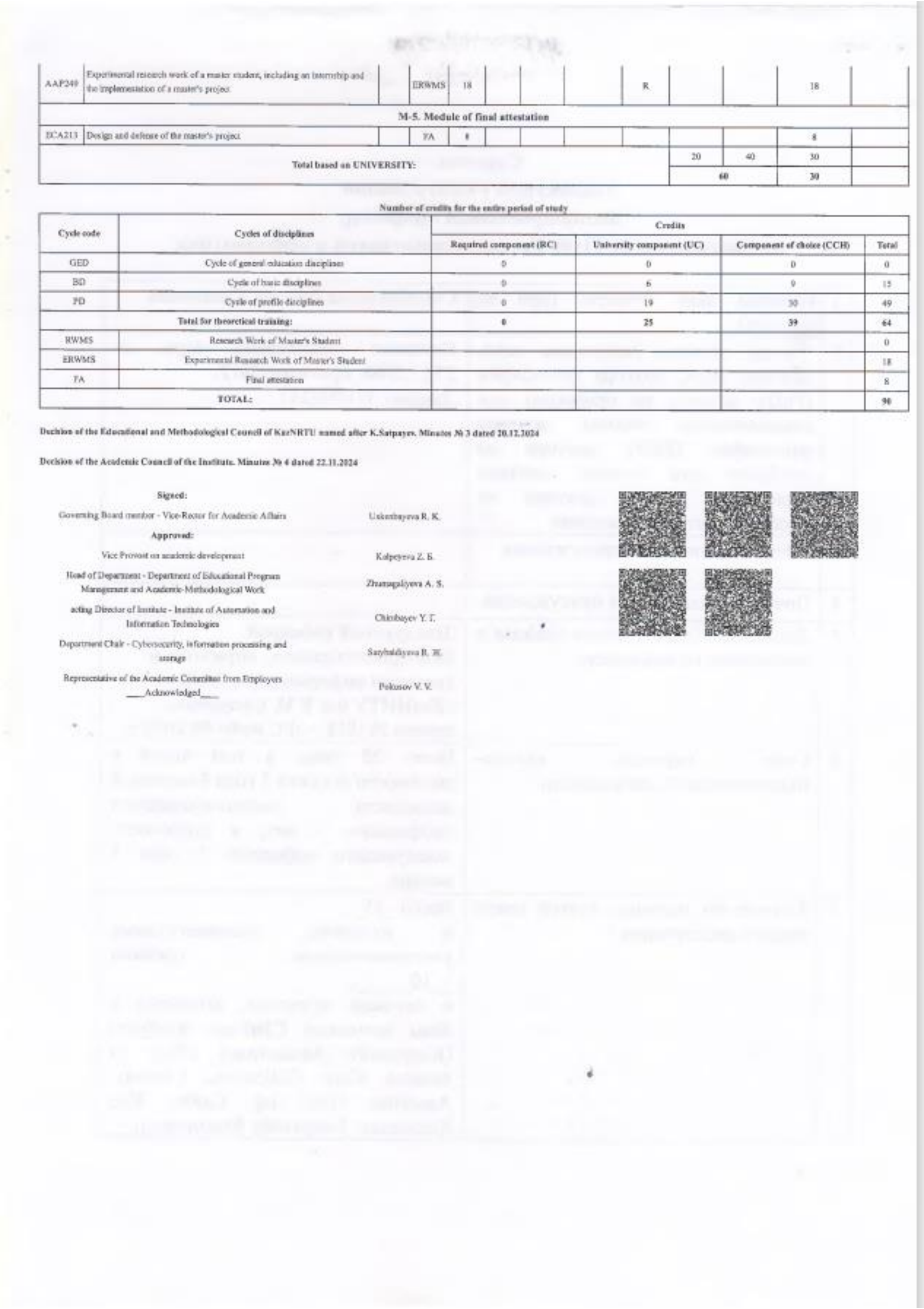
SATBAYEV UNIVERSITY

«APPROVED»
Decision of the Academic Council
NPJSC«KazNRTU
named after K.Satbayev»
dated 06.03.2025 Minutes № 10

WORKING CURRICULUM

Academic year	2025-2026 (Spring, Autumn)
Group of educational programs	M095 - "IT Security"
Educational program	7M06302 - "Comprehensive information security"
The awarded academic degree	Master of engineering and technology
Form and duration of study	full time (professional track) - 1,5 years

Discipline code	Name of disciplines	Block	Cycle	Total ECTS credits	Total hours	lk/lab/pr Contact hours	In hours SIS (including TSIS)	Form of control	Allocation of face-to-face training based on courses and semesters			Prerequisites
									1 course		2 course	
									1 sem	2 sem	3 sem	
CYCLE OF GENERAL EDUCATION DISCIPLINES (GED)												
CYCLE OF BASIC DISCIPLINES (BD)												
M-1. Module of basic training (university component)												
SEC201	Algorithms of cryptographic protection of information	1	BD, CCH	5	150	30/0/15	105	E	5			
SEC210	Methods of cryptology and means of information protection	1	BD, CCH	5	150	30/0/15	105	E	5			SEC121, SEC132
LNG212	Foreign language (professional)		BD, UC	2	60	0/0/30	30	E		2		
MNG726	Management		BD, UC	2	60	15/0/15	30	E		2		
HUM211	Psychology of management		BD, UC	2	60	15/0/15	30	E		2		
SEC257	Security of virtualization and cloud technologies	1	BD, CCH	4	120	30/0/15	75	E		4		
SEC256	Python for solving information security problems	1	BD, CCH	4	120	15/0/30	75	E		4		
CYCLE OF PROFILE DISCIPLINES (PD)												
+	M-2. Module of professional activity (university component, component of choice)											
SEC214	Organization of protection and safety of a database		PD, UC	5	150	30/0/15	105	E	5			
CSE718	Technical protection of information	1	PD, CCH	5	150	15/0/30	105	E	5			
SEC238	Steganographic methods of information protection	1	PD, CCH	5	150	15/0/30	105	E	5			
SEC215	Organization of information security systems		PD, UC	5	150	15/15/15	105	E		5		
SEC246	Big Data and Data Analysis	1	PD, CCH	5	150	30/15/0	105	E		5		
CSE746	Machine Learning & Deep Learning	1	PD, CCH	5	150	30/0/15	105	E		5		
SEC248	Security Internet of things	2	PD, CCH	5	150	15/0/30	105	E		5		
SEC222	Technologies of protection of wireless networks (applications)	2	PD, CCH	5	150	15/0/30	105	E		5		
SEC204	Information Security Audit	3	PD, CCH	5	150	30/0/15	105	E		5		
SEC245	Risk management in cyber security	3	PD, CCH	5	150	30/0/15	105	E		5		
SEC234	OLAP and Data Warehousing	4	PD, CCH	5	150	15/15/15	105	E		5		
CSE258	Data analysis and Data retrieval	4	PD, CCH	5	150	15/15/15	105	E		5		CSE248
SEC240	Cybercrime and computer forensics	5	PD, CCH	5	150	30/0/15	105	E		5		
SEC247	Intellectualized recognition and countermeasures for cyber attacks	5	PD, CCH	5	150	30/0/15	105	E		5		
SEC251	IT project and information risk management		PD, UC	4	120	30/0/15	75	E			4	
M-3. Practice-oriented module												
AAP248	Internship		PD, UC	5				R	5			
M-4.Experimental and research module												



AAP249	Experimental research work of a master student, including an internship and the implementation of a master's project		ERWMS	18				R			18	
M-5. Module of final attestation												
ECA213	Design and defense of the master's project		FA	8							8	
Total based on UNIVERSITY:									20	40	30	
									60		30	

Number of credits for the entire period of study

Cycle code	Cycles of disciplines	Credits			
		Required component (RC)	University component (UC)	Component of choice (CCH)	Total
GED	Cycle of general education disciplines	0	0	0	0
BD	Cycle of basic disciplines	0	6	9	15
PD	Cycle of profile disciplines	0	19	30	49
Total for theoretical training:		0	25	39	64
RWMS	Research Work of Master's Student				0
ERWMS	Experimental Research Work of Master's Student				18
FA	Final attestation				8
TOTAL:					90

Decision of the Educational and Methodological Council of KazNRTU named after K.Satpayev. Minutes № 3 dated 20.12.2024

Decision of the Academic Council of the Institute. Minutes № 4 dated 22.11.2024

Signed:

Governing Board member - Vice-Rector for Academic Affairs	Uskenbayeva R. K.
Approved:	
Vice Provost on academic development	Kalpeyeva Z. B.
Head of Department - Department of Educational Program Management and Academic-Methodological Work	Zhanuzakova A. S.
acting Director of Institute - Institute of Automation and Information Technologies	Chinibayev Y. T.
Department Chair - Cybersecurity, information processing and storage	Satybaldiyeva R. Ж.
Representative of the Academic Committee from Employers ___Acknowledged___	Pokusov V. V.