Ministry of Science and Higher Education of the Republic of Kazakhstan
NJSC «Korkyt Ata Kyzylorda University»

APPROVED
Chairman of the commite
Academic quality
_____ Abzhalelov B.B.
«28» 08 2026 y.

GRADUATE MODEL
of the educational programe 7M06303-«Cybersecurity»

Kyzylorda, 2026

CONTENT

Introduction
1 Description of the OP
2 Components in the formation of the graduate model of the educational program
2.1 Objectives of the Educational program
2.2 Objectives of the Educational Program
2.3 General and professional competencies
2.4 Matrix of correlation of learning outcomes of the educational program with the competencies being formed
2.5 Personal qualities of a social work specialist
Conclusions

INTRODUCTION

The graduate model of Korkyt Ata University is a comprehensive image of the result of studying at the university at all levels of education. The graduate model is recommended for use in the development of educational programs.

The development of a graduate's competence model is an important prerequisite for the implementation of the main directions of the Bologna process and a requirement of the modern labor market. The competence model of a graduate (bachelor) is designed to answer the question of what professional tasks a specialist of a certain rank (position), of a particular profile should be able to solve. The formation of a modern graduate model that meets the needs of all interested parties is the main strategic goal of Korkyt Ata University and is provided with the necessary resources for the educational process, including personnel, educational, methodological, informational and logistical support. The University conducts a targeted personnel policy and systematic improvement of the material and technical base of the university to ensure the quality of training of a bachelor graduate in demand in the labor market.

1. DESCRIPTION DESCRIPTION

The educational program provides training for specialists involved in ensuring the security of systems and network technologies. In particular, he is trained in the field of methods and means of cryptographic information protection, computer technologies for information protection, development and design of cryptographic information protection tools, various methods and means of technical information protection, organization and management of information security services, Organization of computing systems and networks, administration, security of cloud technologies.

2. THE CONSTITUENT COMPONENTS IN THE FORMATION OF THE GRADUATE MODEL OF THE EDUCATIONAL PROGRAM

The key components of the formation of the graduate Model of the educational program include information about the goals and objectives of the educational program, objects, types and directions of professional activity, the competence model of the specialist (Appendix 1), including descriptors, a variety of competencies in accordance with the educational program, the results of the educational program.

2.1 Objectives of the Educational Program:

Training of highly qualified personnel in the field of information security, capable of protecting information at informatization facilities, applying knowledge and personal skills and qualities in ensuring information security. Training of students in general education, basic and specialized disciplines focused on cryptographic and technical protection of information in order to protect and ensure the security of information in various integrated computer systems and networks.

2.2 Objectives of the Educational Program:

- training for the labor market of a new generation of technical specialists in the field of information security with competitive, highly professional competencies;
- integration of educational and scientific activities;
- partnership with leading universities of the near and far abroad in order to improve the quality of education to support technical and cultural ties;

- formation of the practice of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks;
- ensuring the protection of information and computer technology based on network standards and protocols;
- monitoring and analyzing the effectiveness of information security software in operating systems and networks;
- control of the correct operation of hardware and software protection and system administration;
- identification of threats, vulnerabilities and risks in the field of Internet of Things security;
- development, design and support of the organization's network security tools;
- assessment of the security level of the organization's computer systems and networks.

2.3 General and professional competencies

Common:

- Possess the necessary knowledge in the field of information security and understand the possibility of their application in applied fields.

- Know the principles of data processing, analysis and presentation and the ability to apply them in various fields.

- The ability to be competent in choosing ICT and mathematical modeling methods for solving specific engineering problems, the ability to be ready to determine the natural science essence of problems arising in the course of professional activity, and the ability to use the appropriate mathematical apparatus to solve it.

Professional:

- Understanding the architecture of information systems
- The ability to apply theoretical and applied theories and methods
- Management and use of information security standards in the enterprise
- The ability to solve professional problems based on mathematical methods and models for managing IT innovations, computer technologies in the field of information security
- The ability to develop a plan and program for the organization of work on information protection
- The ability to apply mathematical theory and methods to build qualitative and quantitative models of objects and processes in the natural science field
- The ability to choose and apply appropriate equipment, tools and research methods to solve problems in the field of information security, the ability to configure and set up software and hardware complexes in the context of security.

2.1 Matrix of correlation of learning outcomes of the educational program with the competencies being formed

Competencies	LO1	LO2	LO3	LO4	LO5	LO6	LO7	LO8	LO9	LO10
GC1	+									
GC2	+									
GC3	+									
GC4	+									
PC1			+							
PC2		+								
PC3										+
PC4					+					
PC5		+								
PC6						+				

PC7								+		+
PC8						+		+		
PC9										+
PC10							+			
PC11						+				
PC12				+					+	
PC13				+						+
PC14			+	+						
PC15										+

LO1	Knows contemporary theories of the history of science, the methodology of higher education pedagogy, advances in psychological science, and a professional foreign language. Applies modern scientific achievements and educational technologies in solving professional tasks and in the educational process.
LO2	Analyzes cryptographic and steganographic systems, evaluates the cryptographic strength of information protection algorithms, applies modern cryptographic methods, including post-quantum cryptographic algorithms, and uses the analysis results in educational and research activities.
LO3	Designs architectures of secure information systems, computer networks and software complexes, performs threat analysis and justifies the selection of information protection methods and tools to ensure confidentiality, integrity and availability of data in research and educational activities.
LO4	Designs, develops, and maintains secure client-server, cloud, and distributed information systems, including scalable and fault-tolerant cloud architectures; applies containerization, orchestration, microservice architecture, and DevSecOps technologies to ensure software security in research and educational activities.
LO5	Applies modern information security methods in the Internet of Things (IoT) environment, cyber-physical systems, and intelligent infrastructures; uses artificial intelligence technologies to identify threats, analyze security events, assess risks, and enhance the resilience of information systems in educational and research activities.
LO6	Monitors information security events, identifies, analyzes, and investigates incidents using SIEM systems, Big Data technologies, and intelligent data analysis methods (Data Mining and machine learning) for anomaly detection, cyber threat identification, security event correlation, and supporting digital forensics processes in educational and research activities.
LO7	Conducts information security audits, assesses risks and the security level of information systems, plans and organizes audit activities, applies international audit standards and methodologies, and develops recommendations for improving information security management systems in research and educational activities.
LO8	Designs and implements identification, authentication, authorization, and access control mechanisms; applies modern access control models and digital identity management technologies to ensure the security of information systems in research and educational activities.
LO9	Applies distributed ledger technologies (blockchain) to ensure integrity, authenticity, and trust in information processing; analyzes their potential use to enhance the security of digital services and information systems in educational and research activities.
LO10	Applies modern methods for detecting, analyzing, and countering malicious software; uses static and dynamic code analysis methods, artificial intelligence technologies, machine learning, and modeling techniques to identify, classify,

	assess, and predict cyber threats in professional, research, and educational activities.

2.4 Personal qualities of an information security specialist

-Analytical skills: conducting a systematic analysis of information; systematization of information; data comparison; abstracting information; designing the result.
-Diagnostic skills: the ability to structure the information received; implement innovative and combinational processes related to the ability to predict; determine strategic, tactical and operational goals; formulate and solve professional tasks; use positive experience; make managerial decisions; diagnose possible solutions.
-Verbal and non-verbal skills: establishing business relationships with colleagues; cooperation with partners; formulation of professional tasks; mastering oral and written speech; solving non-standard tasks using methods and tools; determining significance in extreme situations.
-Forecasting skills: confidence in their actions in accordance with the assessment of everything that is happening; determination, management, information modeling, energy mobilization, perseverance, activity, ability to bear the load, as a condition of perseverance in performing complex tasks.
-Correctional skills: self-analysis, self-correction; determination of trajectories of self-development and self-education; understanding of one's professional and personal capabilities.

Types of professional activity of a bachelor in the field of information and communication technologies under the educational program 6B06352-"Information security systems":
- Information security auditor
- Information Security Engineer
- Information Security Administrator
- System administrator
- Specialist of the Information security Service
- Database Analyst
- Research associate
- Heads of services and departments in the field of information and communication technologies and information security.

CONCLUSIONS

In market conditions, universities are beginning to pay more attention to the quality of graduates: a graduate is the result of university education entering the labor market. And it has to be competitive. To prepare graduates in demand on the market, it is necessary to form a comprehensive portrait of him, a certain matrix of characteristics. The formation of educational programs with an understanding of the main advantages, characteristics, competencies of graduates needed by employers, the creation of infrastructure, the transition to the creation of an effective modern university based on the use of new learning formats.

Appendix 1

The graduate's competence model

Module	DDB (Dublin Descriptors of bachelor)	Emerging competencies			Planned learning outcomes
		general education competencies	basic competencies	professional competencies	
1	2	3	4	5	6
M1	DDB1 DDB2 DDB3 DDB4 DDB5	GC1			LO1 Knows contemporary theories of the history of science, the methodology of higher education pedagogy, advances in psychological science, and a professional foreign language. Applies modern scientific achievements and educational technologies in solving professional tasks and in the educational process.
	DDB1 DDB2 DDB3 DDB4 DDB5	GC2			LO1 Knows contemporary theories of the history of science, the methodology of higher education pedagogy, advances in psychological science, and a professional foreign language. Applies modern scientific achievements and educational technologies in solving professional tasks and in the educational process.
	DDB1 DDB2 DDB3 DDB4 DDB5	GC3			LO1 Knows contemporary theories of the history of science, the methodology of higher education pedagogy, advances in psychological science, and a professional foreign language. Applies modern scientific achievements and educational technologies in solving professional tasks and in the educational process.
	DDB1 DDB2 DDB3 DDB4	GC4			LO1 Knows contemporary theories of the history of science, the methodology of higher education pedagogy, advances in psychological science, and a professional foreign language. Applies modern scientific achievements and educational technologies in solving professional tasks and in the educational process.

	DDB5				
M1	DDB1 DDB2 DDB3 DDB4 DDB5			PC1	LO3 Designs architectures of secure information systems, computer networks and software complexes, performs threat analysis and justifies the selection of information protection methods and tools to ensure confidentiality, integrity and availability of data in research and educational activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC2	LO2 Analyzes cryptographic and steganographic systems, evaluates the cryptographic strength of information protection algorithms, applies modern cryptographic methods, including post-quantum cryptographic algorithms, and uses the analysis results in educational and research activities.
M2	DDB1 DDB2 DDB3 DDB4 DDB5			PC4	LO5 Applies modern information security methods in the Internet of Things (IoT) environment, cyber-physical systems, and intelligent infrastructures; uses artificial intelligence technologies to identify threats, analyze security events, assess risks, and enhance the resilience of information systems in educational and research activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC5	LO2 Analyzes cryptographic and steganographic systems, evaluates the cryptographic strength of information protection algorithms, applies modern cryptographic methods, including post-quantum cryptographic algorithms, and uses the analysis results in educational and research activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC6	LO6 Monitors information security events, identifies, analyzes, and investigates incidents using SIEM systems, Big Data technologies, and intelligent data analysis methods (Data Mining and machine learning) for anomaly detection, cyber threat identification, security event correlation, and supporting digital forensics processes in educational and research activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC7	LO8 Designs and implements identification, authentication, authorization, and access control mechanisms; applies modern access control models and digital identity management technologies to ensure the security of information systems in research and educational activities. LO10 Applies modern methods for detecting, analyzing, and countering malicious software; uses static and dynamic code analysis methods, artificial intelligence technologies, machine learning, and modeling

					techniques to identify, classify, assess, and predict cyber threats in professional, research, and educational activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC8	LO6 Monitors information security events, identifies, analyzes, and investigates incidents using SIEM systems, Big Data technologies, and intelligent data analysis methods (Data Mining and machine learning) for anomaly detection, cyber threat identification, security event correlation, and supporting digital forensics processes in educational and research activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC10	LO7 Conducts information security audits, assesses risks and the security level of information systems, plans and organizes audit activities, applies international audit standards and methodologies, and develops recommendations for improving information security management systems in research and educational activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC11	LO6 Monitors information security events, identifies, analyzes, and investigates incidents using SIEM systems, Big Data technologies, and intelligent data analysis methods (Data Mining and machine learning) for anomaly detection, cyber threat identification, security event correlation, and supporting digital forensics processes in educational and research activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC12	LO4 Designs, develops, and maintains secure client-server, cloud, and distributed information systems, including scalable and fault-tolerant cloud architectures; applies containerization, orchestration, microservice architecture, and DevSecOps technologies to ensure software security in research and educational activities. LO9 Applies distributed ledger technologies (blockchain) to ensure integrity, authenticity, and trust in information processing; analyzes their potential use to enhance the security of digital services and information systems in educational and research activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC13	LO4 Designs, develops, and maintains secure client-server, cloud, and distributed information systems, including scalable and fault-tolerant cloud architectures; applies containerization, orchestration, microservice architecture, and DevSecOps technologies to ensure software security in research and educational activities. LO10 Applies modern methods for detecting, analyzing, and countering malicious software; uses static and

					dynamic code analysis methods, artificial intelligence technologies, machine learning, and modeling techniques to identify, classify, assess, and predict cyber threats in professional, research, and educational activities.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC14	LO3 Designs architectures of secure information systems, computer networks and software complexes, performs threat analysis and justifies the selection of information protection methods and tools to ensure confidentiality, integrity and availability of data in research and educational activities. LO4 Designs, develops, and maintains secure client-server, cloud, and distributed information systems, including scalable and fault-tolerant cloud architectures; applies containerization, orchestration, microservice architecture, and DevSecOps technologies to ensure software security in research and educational activities.
M3	DDB1 DDB2 DDB3 DDB4 DDB5			PC3	LO10 Knows modern methods and technologies for ensuring information security, as well as the principles of protecting information systems and computer networks. Has a command of methods for analyzing cyber threats, assessing risks, and identifying vulnerabilities. Applies modern cybersecurity technologies and scientific research findings to solve professional tasks.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC9	LO10 Knows modern scientific research methods in the field of information security, as well as the principles of cyberattack detection and information system security assessment. Has a command of experimental research methods, network traffic analysis, and data processing techniques. Applies machine learning algorithms, neural networks, and modern cybersecurity tools to detect threats, predict attacks, and enhance the security of information systems.
	DDB1 DDB2 DDB3 DDB4 DDB5			PC15	LO10 Knows modern methods and technologies of information protection, the principles of operation of secure computer systems and networks, and methods for assessing their reliability and security. Possesses skills in conducting scientific experiments, analyzing vulnerabilities, and investigating network threats. Applies artificial intelligence, machine learning, and data analysis methods to identify cyberattacks, detect anomalies, and develop effective information protection mechanisms.

M1 - Sciense knowledge
M2 - Sciense (by industry) and innovation
M3 - The final assessment