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

I APPROVE
Chairman of the commite
Academic quality
«1» 09.08 2024 y.

GRADUATE MODEL

Bachelor's degree in the educational programm
6B06352-«Information security systems»

Kyzylorda, 2024

CONTENT

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	LO 2	LO 3	LO 4	LO 5	LO 6	LO 7	LO 8
GEC 1	+							
GEC 2	+							
GEC 3	+							
GEC 4	+							
GEC 5	+							
GEC 6		+	+					
GEC 7	+							
GEC 8	+							
SC1	+	+						
SC2	+	+						
SC3			+	+	+			
SC4	+	+						
SC5	+		+					
SC6			+					
SC7			+	+	+			
SC8		+						
SC9			+		+			
SC10	+	+						
SC11			+					
SC12		+						
SC13			+					
SC14			+	+	+			
SC15					+			
SC16		+						
SC17					+			
SC18 Minor		+						
SC19 Minor			+	+	+			
SC20	+							+
SC21		+						+
SC22	+							
SC23			+	+	+			
SC24					+	+		
SC25					+			
SC26			+			+		
SC27				+				
PC1				+				
PC2			+					
PC3							+	+
PC4					+		+	+
PC5			+					
PC6						+		+
PC7			+		+			
PC8						+	+	
PC9 Minor				+				

LO1	Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security
LO2	Apply theoretical and practical knowledge in the field of natural sciences and mathematics to solve professional problems and modeling processes in the field of information security. Knowledge of the principles of the theory of electrical circuits and digital signal processing.
LO3	Demonstrate knowledge about the element base, architecture, operating systems of computer systems, networks and organizations and ensuring their security, setting up the security policy of operating systems, DBMS, programming technologies and methods to protect information and information processes
LO4	Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security
LO5	Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
LO6	Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents.
LO7	Apply theoretical knowledge and practical skills for the functioning of vulnerability monitoring systems, information security event management systems and information leak prevention systems.
LO8	Apply knowledge in the field of design and secure software development for verification, static analysis and identification of software code vulnerabilities. Apply knowledge of the principles of safe use and protection of cloud technologies, demonstrate knowledge and skills in the field of big data security

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	GEC 1, GEC 2, GEC3, GEC 4, GEC 5			LO1 Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security
M1	DDB1 DDB2 DDB3 DDB4 DDB5	GEC 6			LO2 Apply theoretical and practical knowledge in the field of natural sciences and mathematics to solve professional problems and modeling processes in the field of information security. Knowledge of the principles of the theory of electrical circuits and digital signal processing. LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.
	DDB1 DDB2 DDB3 DDB4 DDB5	GEC7, GEC 8			LO1 Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security
M3	DDB1 DDB2 DDB3 DDB4 DDB5		SC1, SC2, SC4, SC10		LO1 Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security LO2 Apply theoretical and practical knowledge in the field of natural sciences and mathematics to solve professional problems and

					modeling processes in the field of information security. Knowledge of the principles of the theory of electrical circuits and digital signal processing.
	DDB1 DDB2 DDB3 DDB4 DDB5		SC3, SC7		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes. LO4 Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
M2	DDB1 DDB2 DDB3 DDB4 DDB5		SC5		LO1 Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.
	DDB1 DDB2 DDB3 DDB4 DDB5		SC6		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.
M3	DDB1 DDB2 DDB3 DDB4 DDB5		SC8 SC12		LO2 Apply theoretical and practical knowledge in the field of natural sciences and mathematics to solve professional problems and modeling processes in the field of information security. Knowledge of the principles of the theory of electrical circuits and digital signal processing.
M5	DDB1 DDB2 DDB3 DDB4		SC9		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.

	DDB5				LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
M4	DDB1 DDB2 DDB3 DDB4 DDB5		SC11S C13		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.
M5	DDB1 DDB2 DDB3 DDB4 DDB5		SC14		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes. LO4 Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
M4	DDB1 DDB2 DDB3 DDB4 DDB5		SC15 SC17		LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
	DDB1 DDB2 DDB3 DDB4 DDB5		SC16 SC18		LO2 Apply theoretical and practical knowledge in the field of natural sciences and mathematics to solve professional problems and modeling processes in the field of information security. Knowledge of the principles of the theory of electrical circuits and digital signal processing.
	DDB1 DDB2 DDB3		SC19		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.

	DDB4 DDB5				LO4 Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
M6	DDB1 DDB2 DDB3 DDB4 DDB5		SC20		LO1 Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security LO8 Apply knowledge in the field of design and secure software development for verification, static analysis and identification of software code vulnerabilities. Apply knowledge of the principles of safe use and protection of cloud technologies, demonstrate knowledge and skills in the field of big data security
M5	DDB1 DDB2 DDB3 DDB4 DDB5		SC21		LO2 Apply theoretical and practical knowledge in the field of natural sciences and mathematics to solve professional problems and modeling processes in the field of information security. Knowledge of the principles of the theory of electrical circuits and digital signal processing. LO8 Apply knowledge in the field of design and secure software development for verification, static analysis and identification of software code vulnerabilities. Apply knowledge of the principles of safe use and protection of cloud technologies, demonstrate knowledge and skills in the field of big data security
M6	DDB1 DDB2 DDB3 DDB4 DDB5		SC22		LO1 Demonstrate the ability and willingness to apply knowledge in the natural science, humanitarian, socio-economic, and entrepreneurial fields. Knowledge of the basic requirements of international and national legislative, organizational and procedural acts regulating activities in the field of Information Security
M5	DDB1 DDB2 DDB3 DDB4 DDB5		SC23		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes. LO4 Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security

					LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
	DDB1 DDB2 DDB3 DDB4 DDB5		SC24		LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems. LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents.
M3	DDB1 DDB2 DDB3 DDB4 DDB5		SC25		LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
M5	DDB1 DDB2 DDB3 DDB4 DDB5		SC26		LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes. LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents.
M6	DDB1 DDB2 DDB3 DDB4 DDB5		SC27		LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents.
M4	DDB1 DDB2 DDB3 DDB4 DDB5			PC 1	LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents.
M5	DDB1			PC2	LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and

	DDB2 DDB3 DDB4 DDB5				ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.
M6	DDB1 DDB2 DDB3 DDB4 DDB5			PC 3 PC11	LO7 Apply theoretical knowledge and practical skills for the functioning of vulnerability monitoring systems, information security event management systems and information leak prevention systems. LO8 Apply knowledge in the field of design and secure software development for verification, static analysis and identification of software code vulnerabilities. Apply knowledge of the principles of safe use and protection of cloud technologies, demonstrate knowledge and skills in the field of big data security
M5	DDB1 DDB2 DDB3 DDB4 DDB5			PC 4	LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems. LO7 Apply theoretical knowledge and practical skills for the functioning of vulnerability monitoring systems, information security event management systems and information leak prevention systems. LO8 Apply knowledge in the field of design and secure software development for verification, static analysis and identification of software code vulnerabilities. Apply knowledge of the principles of safe use and protection of cloud technologies, demonstrate knowledge and skills in the field of big data security
M6	DDB1 DDB2 DDB3 DDB4 DDB5			PC 5	LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes.
M7	DDB1 DDB2 DDB3 DDB4 DDB5			PC 6	LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents. LO8 Apply knowledge in the field of design and secure software development for verification, static analysis and identification of software code vulnerabilities. Apply knowledge of the principles of safe use and protection of cloud technologies, demonstrate knowledge and skills in the field of big data security
M6	DDB1 DDB2			PC 7	LO3 Demonstrate knowledge about the architecture of operating systems, computer systems and networks and the organization and

	DDB3 DDB4 DDB5				ensuring their security, setting up a DBMS security policy, programming technologies and methods to protect information and information processes. LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems.
M6	DDB1 DDB2 DDB3 DDB4 DDB5			PC 8	LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents. LO7 Apply theoretical knowledge and practical skills for the functioning of vulnerability monitoring systems, information security event management systems and information leak prevention systems.
M7	DDB1 DDB2 DDB3 DDB4 DDB5			PC 9	LO4 Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security
M7	DDB1 DDB2 DDB3 DDB4 DDB5			PC10	LO4 Demonstration of knowledge in the field of information theory and coding and cryptology, knowledge of mathematical principles of cryptography algorithms and other methods of information concealment. Ability to choose and use software and hardware to ensure information security LO5 Applies the principles of construction and types of architecture of artificial intelligence systems. Interacts with organizational units as part of the application design process, database structure, and software interfaces. He knows the basic tools of artificial intelligence, as well as methods and means of verifying the operability of artificial intelligence systems. LO6 Apply knowledge, understanding of facts, complex dependencies in the field of malware detection, in the field of practical pentesting and investigation of computer incidents.