NAO "KAZAKH NATIONAL RESEARCH TECHNICAL UNIVERSITY
named after K.I. SATPAYEV"

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

EDUCATIONAL PROGRAM

"7M06301 - Integrated information security"

(the cipher and the name of the educational program)

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: 2 years
Volume of credits: 120 credits

Almaty 2025

The educational program "7M06301 - 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.
Протокол № __3__ от "__20__" ___12_____2024.

The educational program "7M06301 - Integrated information security" was developed by the academic committee in the direction "7M063 Information security"

Ф.И.О.	Last name first name patronymic	Post	Place of work	Signature
Chairman of the Academic Committee:				
Pokusov Viktor Vladimirovich		Chairman	Kazakhstan Information Security Association	
Academic staff:				
Aitkhozhaeva Evgeniya Zhamalkhanovna	Candidate of Technical Sciences, Associate Professor	Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Rakhmetulayeva Sabina Batyrkhanovna	PhD	Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Satybaldiyeva Ryshan Zhakanovna	Candidate of Technical Sciences,	Associate Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Serbin Vasily Valerievich	Candidate of Technical Sciences,	Associate Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Zhumagaliev Birzhan Izimovich	Candidate of Technical Sciences, Associate Professor	Associate Professor	NJSC "KazNRTU named after K.I. Satpaev"	
Alimseitova Zhuldyz Keneskhanovna	Doctor of PhD	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:				
Mamyrbayev Orken Zhumazhanovich	Doctor of PhD Associate Professor	Deputy Director General	RSE "Institute of Information and Computing Technologies"	
Konysbayev Amret Tuyakuly	Candidate of Physico-mathematical Sciences	President	Association of Innovative Companies of the FEZ "PIT"	
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

1. Description of the educational program

The educational program is aimed at training undergraduates in 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 in the scientific and pedagogical field of information security will be carried out according to the updated educational program "Integrated Information Security". The programs of the 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 activity in the field of information security within the framework of the ESG and the Sustainable Development Goals (SDGs).

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 "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. The purpose and objectives of the educational program

Purpose of the OP:

The purpose of the educational program is to train specialists in the field of infocommunication technologies and information security technologies (electronic digital signature, identification infrastructure, protection of network protocols, antivirus protection, content filtering, etc.).

OP tasks:

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 information security of the object of information security audit;
- analysis of the current security status of the IB audit object;
- identification and elimination of vulnerabilities;
- monitoring and investigation of information security incidents;
- development of a model of information security threats in enterprises;
- development of technical specifications for the creation of an information security system.

The Master of the educational program "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 the evaluation of learning outcomes of the educational program

The requirements for the master's degree level are determined on the basis of the Dublin descriptors of the second level of higher education (Master's degree) and reflect the acquired competencies expressed in the achieved learning outcomes.
Learning outcomes are formulated both at the level of the entire master's degree program and at the level of individual modules or academic discipline.

A graduate who has mastered master's degree programs must have the following general professional competencies:

the ability to independently acquire, comprehend, structure and use new knowledge and skills in professional activities, develop their innovative abilities;

– the ability to independently formulate research goals, establish the sequence of solving professional tasks;

– the ability to apply in practice the knowledge of fundamental and applied sections of disciplines that determine the orientation (profile) of the master's degree program;

– the ability to professionally choose and creatively use modern scientific and technical equipment to solve scientific and practical problems;

– the ability to critically analyze, present, defend, discuss and disseminate the results of their professional activities;

– proficiency in the preparation and execution of scientific and technical documentation, scientific reports, reviews, reports and articles;

– willingness to lead a team in the field of their professional activities, tolerantly perceiving social, ethnic, confessional and cultural differences;

– readiness to communicate orally and in writing in a foreign language to solve the tasks of professional activity.

A graduate who has mastered the master's degree program must have professional competencies corresponding to the types of professional activities that the master's degree program is focused on:

research activities:

– the ability to form diagnostic solutions to professional problems by integrating the fundamental sections of sciences and specialized knowledge obtained during the development of the master's degree program;

– the ability to independently conduct scientific experiments and research in the professional field, generalize and analyze experimental information, draw conclusions, formulate conclusions and recommendations;

– the ability to create and explore models of the studied objects based on the use of in-depth theoretical and practical knowledge in the field of information protection and security;

– scientific and production activity:

- the ability to independently carry out production and scientific–production, laboratory and interpretive work in solving practical problems;

– the ability to professionally operate modern laboratory equipment and devices in the field of the master's degree program;

– the ability to use modern methods of processing and interpreting complex information to solve production problems;

– project activities:

– the ability to independently compile and submit projects of research and scientific-production works in the field of information security;

– readiness to design complex research and scientific-production works in solving professional tasks;

– organizational and managerial activity:

- readiness to use practical skills in organizing and managing research and scientific-production works in solving professional tasks;

– readiness for the practical use of regulatory documents in the planning and organization of scientific and production work in the field of information security

scientific and pedagogical activity:

- ability to conduct seminars, laboratory and practical classes;

– the ability to participate in the management of scientific and educational work of students in the field of information security.

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	7M06301 - Integrated information security
5	Brief description of the educational program	The professional activities of graduates include: science, education, state and departmental structures, the economy and industry of the state, the field of healthcare. The objects of professional activity of graduates of master's degree programs in the educational program - "Integrated information security" are: − 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. 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, 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	The purpose of the Educational program	Training of specialists in the field of infocommunication technologies and information security technologies (electronic digital signature, identification infrastructure, protection of network protocols, antivirus protection, content filtering, etc.).
7	Type of educational program	Updated educational program
8	The level of the NRK	7
9	ORC Level	7
10	Distinctive features of the Educational program	The program is focused on training professional specialists in the field of information security management. Unlike the existing educational programs in the field of information security, it is

		planned to actively expand the graduate's training towards the use of world practice and information security standards, which will provide him with advanced training.
11	List of competencies of the 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; – information security 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 building hypervisors and their vulnerabilities; – 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. 3) be able to: – to 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; – to summarize the results of research and analytical work in the form of a dissertation, a scientific article, a report, an analytical note, etc.; - to 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; – organize a database protection and security system; – apply methods and tools of active audit; – apply big data analysis tools. 4) have skills: – 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 information security 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. 5) be competent: – 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 information security systems; – in 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 Have the ability to formulate research goals independently, establish the sequence of solving professional tasks. ON2 Have professional competencies to create and research a model of the objects under study based on the use of in-depth theoretical and practical knowledge in the field of information security and security. ON 3 The ability to design complex research and scientific-production works in solving professional problems. Proficiency in foreign languages at a professional level. ON 4 Readiness for the practical use of regulatory documents in the planning and organization of scientific and production work in the field of information security. To know the current and promising trends in the development of cryptographic information protection and apply it in practice. ON 5 Understand philosophical questions of science, the main historical stages of the development of science, be able to critically evaluate and analyze scientific and philosophical problems, understand the specifics of engineering science, possess analytical

		thinking skills.Be competent in psychology and pedagogy. ON 6 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. ON 7 Be able to assess the security of network operating systems. It is safe to use modern virtualization technologies. Know and apply methods and tools for conducting an information security audit. ON 8 Ability to design complex scientific research and scientific production works while solving professional tasks. Proficiency in foreign languages at a professional level for partnership for sustainable development ON 9 Know the technical means and methods of technical protection of information, be competent in the organization of engineering and technical protection of information. ON 10 Be able to analyze big data, know the methods and tools of big data analysis. Ability to formulate problems, tasks and methods of scientific research.
13	Form of training	full - time
14	Duration of training	2 years
15	Volume of loans	120 credits
16	Languages of instruction	Kazakh, Russian,
17	Academic degree awarded	Master of Technical Sciences
18	Developer(s) and authors:	Aitkhozhaeva E.Zh., Begimbayeva E.E., Satybaldieva R.Zh., Yubuzova H.I.

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**	**ON6**	**ON7**	**ON8**	**ON9**	**ON10**
The cycle of basic disciplines The university component													
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 tables, debates, discussions, analysis of professionally oriented cases, design).	3			v					v		
2	History and philosophy of science	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, nonclassical and post-nonclassical science, philosophy of mathematics, physics, engineering and technology, specifics of engineering sciences, ethics of science, social and moral responsibility of scientists and engineers.	3	v			v						v
3	Higher school pedagogy	During the course, undergraduates will master the methodological and theoretical foundations of higher school pedagogy, learn how to use modern pedagogical technologies, plan and organize learning and upbringing processes, and master the communicative technologies of subject-subject interaction between a teacher and a graduate student in the educational process of a university. Undergraduates also study human resource management in educational organizations (using the example of higher education).	3	v			v						v

4	Psychology of management	The discipline studies the modern role and content of psychological aspects in management activities. The article considers the improvement of psychological literacy of the student in the process of professional activity. He improves himself in the field of psychology and studies the composition and structure of management activities, both at the local level and abroad. The psychological feature of modern managers is considered.	3	v								v	v
The cycle of basic disciplines Component of choice													
5	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		v				
6	Security of virtualization and cloud technology systems	During the course, the issues of cloud technology security and sources of threats in cloud computing will be considered. Cloud deployment models will be studied: 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		v					
7	Intellectual property and scientific research	The aim of this course is to provide undergraduates with the knowledge and skills necessary to understand, protect, and manage intellectual	5	v	v								v

		property (IP) in the context of scientific research and innovation. The course is aimed at training specialists who are able to work effectively with IP, protect the results of scientific research and apply them in practice.											
8	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**			**v**	
9	Methods and means of protection in the OS	The course covers protection against modification and software integrity control. Methods and means of storing key information. Principles of multi-factor authentication. Technical identification and authentication devices. Software and hardware encryption tools. Ensuring security in Windows and 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	Network OS security features	Fundamentals of network security. Integrated software monitoring and protection against software corruption. Principles of multipath authentication. Identification and authentication of technical devices. Secure identification and authentication subsystems. Identification and authentication of users using biometric devices. Software and hardware encryption. Security of network operating	5		**v**		**v**			**v**			

		systems. Security in Windows, Unix. Dirt detection systems. The main components of the firewall architecture. Modern requirements for firewalls.											
11	Sustainable development strategies	The aim of this course is to provide undergraduates with in-depth knowledge and practical skills to develop, implement and manage strategies aimed at achieving sustainable development. The course content covers the following topics: fundamentals of sustainable development, economic aspects of sustainable development, social aspects of sustainable development, development of sustainable development strategies, innovation and technology in sustainable development, ethics and sustainable development, prospects and future of sustainable development.	5	v	v								v
12	Python in research activities	The course examines the general principles of working with data: loading, receiving and processing unstructured data, receiving data through API, Visualization and publication of data, filtering, transformation, analysis and interpretation of data using well-known models of classification, clustering, regression, etc. The range of tasks covers optimization methods, stochastic modeling, Gaussian modeling, partial differential equations, the Navier-Stokes equation, and the equations of thermal conductivity.	5	v		v							
The cycle of profile disciplines The university component													
13	Quantum information security technologies	The purpose of studying the discipline is to apply the principles of quantum mechanics in order to ensure the security and protection of information. Students study the principles of quantum cryptographic protocols, quantum cryptanalysis and methods of protection against attacks, as well as various quantum technologies used in the field of information security. The course also covers current topics related to the development of quantum	4				v		v			v	

		computers and their potential impact on cryptographic systems.											
14	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 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.	5	v		v							v
15	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						
The cycle of profile disciplines Component of choice													
16	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 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	5				v						

		be covered.											
17	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**					
18	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. 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.	5	**v**					**v**		**v**		
19	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**			**v**			
20	Artificial intelligence	The goal of artificial intelligence is to create technical systems capable of solving non-	5		**v**		**v**						**v**

		computational tasks and performing actions that require processing meaningful information and are considered the prerogative of the human brain.											
21	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			
22	Natural language processing	The course examines 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 text processing. Classical algorithms for processing text information are considered, such as regular expressions, measuring distances, substitutions, searching for strings and substrings. Linguistic trees. The body of the text. Taxonomy. The models of Word2Vec, Text Embedding, and LSTM neural network models are considered. The existing libraries of text information analysis are being studied.	5		v	v						v	v
23	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	
24	Steganographic methods of information	The content of the discipline covers a range of issues related to the protection of information through mathematical transformations using steganographic	5		v					v		v	

	protection	algorithms and copyright protection algorithms.											
25	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			
26	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		v				
27	Machine Learning & Deep Learning	The course focuses on deep learning models. As an area within machine learning, deep learning models illustrate the quantitative-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.	5			v	v						v
28	OLAP and data warehouses	The purpose of mastering the discipline is to gain in-depth knowledge about data storage systems and	5				v	v					v

		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.											
29	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**	**v**				

5. Curriculum of the educational program