МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи
_____
Каріна НЕМАЩКАЛО

ТЕОРЕТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***англійська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2021

MINISTRY (ION AND SCIENCE OF UKRAINE
SIMON KUZNETS KH. . .ATIONAL UNIVERSITY OF ECONOMICS

"APPROVED"
Vice-rector for educational and methodical work
Karina NEMASHKALO

THEORETICAL FUNDAMENTALS OF CRYPTOGRAPHY

working program of the discipline

Field of knowledge	***12 Information technologies***
Speciality	***125 Cybersecurity***
Educational level	***first (bachelor's)***
Educational program	***Cybersecurity***

Discipline status	***basic***
Language of instruction, teaching and assessment	***English***

Head of Department
cybersecurity and
information technology Serhii YEVSEIEV

Kharkiv
2021

APPROVED
at a meeting of the *Department of Cybersecurity and Information Technology*
Protocol № 1 dated 27.08.2021

Developer:
Milov O.V., D.Sc., Prof. of CIT Department.

Update and re-approval letter
working program of the discipline

Academic year	Date of the meeting of the department-developer of WP	Protocol number	Signature of the head of the department

Abstract of the discipline

The discipline "Theoretical fundamentals of cryptography" is basic in the preparation of bachelors in accordance with the curriculum of the specialty "Cybersecurity", and is aimed at acquainting students with the basics of the theory of binary coding, noise-tolerant coding. The discipline "Theoretical foundations of cryptography" is considered as a theoretical and applied discipline that gives an idea of the basic mathematical and algorithmic approaches used to store, transmit, correct information presented in binary codes. The course is devoted to the study of the basics of cryptography and cryptographic analysis used to protect information in information systems, introduces students to the concept of ciphers, symmetric and asymmetric cryptography, electronic signature, hashing and other mathematical objects of cryptography. Relevant cryptographic standards used today to protect information in Ukraine and abroad are being studied. RSA, DES, GOST1989 and other standards are considered in detail. Attention is also paid to promising areas in cryptography: cryptographic protocols with and without disclosure, the theory of algorithmic complexity and one-sided functions, secret sharing schemes and some of their application in the problems of identification and authentication.

The purpose of the discipline is to get acquainted with the theoretical foundations of cryptology, acquire skills in practical use, formulation and solution of information encryption, understanding the essence of information processes in cryptographic systems, use of computers to solve encryption and decryption, development and use of mathematical and computational process models encryption of information, their optimization and development of areas for improvement.

Characteristics of the discipline

Course	**2**
Semester	**3**
Number of ECTS credits	**5**
Form of final control	**exam**

Structural and logical scheme of studying the discipline

Prerequisites	**Postrequisites**
Entry to the profession	Programming technologies
Programming	Fundamentals of cryptographic protection
Mathematical foundations of cryptology	

Competences and learning outcomes in the discipline

Competences	Learning outcomes
OC 1. Ability to apply knowledge in practical situations.	LO 1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication; LO 2 - to organize their own professional activities, choose the best methods and ways to solve complex specialized problems and practical problems in professional activities, evaluate their effectiveness; LO 3 - use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity; LO 4 - analyze, argue, make decisions in solving complex specialized problems and practical problems in professional activities, which are characterized by complexity and incomplete definition of conditions, be responsible for the decisions made; LO 10 - perform analysis and decomposition of information and telecommunication systems; LO 11 - perform analysis of connections between information processes on remote computer systems; LO 18 - use software and software and hardware systems for the protection of information resources;

	LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 21 - to solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information and information and telecommunications (automated) systems; LO 22 - to solve problems of management of procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and / or cybersecurity; LO 24 - to solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role); LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems; LO 32 - to solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity; LO 53 - to solve problems of analysis of program code for the presence of possible threats; LO 54 - to be aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.
OC 2. Knowledge and understanding of the subject area and understanding of the profession.	LO 1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication; LO 2 - to organize their own professional activities, choose the best methods and ways to solve complex specialized problems and practical problems in professional activities, evaluate their effectiveness; LO 3 - use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity; LO 4 - analyze, argue, make decisions in solving complex specialized problems and practical problems in professional activities, which are characterized by complexity and incomplete definition of conditions, be responsible for the decisions made; LO 5 - to adapt to frequent changes in the technology of professional activity, to predict the end result; LO 6 - critically comprehend the basic theories, principles, methods and concepts in teaching and professional activities; LO 7 - to act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and / or cybersecurity; LO 8 - prepare proposals for regulations to ensure information and / or cybersecurity; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural

	(structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 54 - to be aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.
OC 3. Ability to communicate professionally in state and foreign languages both orally and in writing.	LO 1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication
OC 4. Ability to identify, pose and solve problems in a professional direction.	LO 2 - to organize their own professional activities, choose the best methods and ways to solve complex specialized problems and practical problems in professional activities, evaluate their effectiveness; LO 3 - use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity; LO 4 - analyze, argue, make decisions in solving complex specialized problems and practical problems in professional activities, which are characterized by complexity and incomplete definition of conditions, be responsible for the decisions made; LO 5 - to adapt to frequent changes in the technology of professional activity, to predict the end result; LO 7 - to act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and / or cybersecurity; LO 8 - prepare proposals for regulations to ensure information and / or cybersecurity; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
OC 5. Ability to search, process and analyze information.	LO 2 - to organize their own professional activities, choose the best methods and ways to solve complex specialized problems and practical problems in professional activities, evaluate their effectiveness; LO 3 - use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity; LO 4 - analyze, argue, make decisions in solving complex specialized problems and practical problems in professional activities, which are characterized by complexity and incomplete definition of conditions, be responsible for the decisions made; LO 5 - to adapt to frequent changes in the technology of professional activity, to predict the end result; LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 28 - to analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during tests in accordance with the established policy of information and / or cybersecurity.
OC 6. Ability to exercise their rights and responsibilities as a member of society, to realize the values of civil (free democratic) society and the need for its sustainable	LO 54 - to be aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.

development, the rule of law, human and civil rights and freedoms in Ukraine.	
OC 7. Ability to preserve and increase moral, cultural, scientific values and achievements of society based on understanding the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, techniques and technologies, use different types and forms physical activity for active recreation and a healthy lifestyle.	LO 54 - to be aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.
PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and / or cybersecurity.	LO 7 - to act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and / or cybersecurity; LO 8 - prepare proposals for regulations to ensure information and / or cybersecurity; LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents; LO 34 - to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards.
PC 2. Ability to use information and communication technologies, modern methods and models of information security and / or cybersecurity.	LO 10 - perform analysis and decomposition of information and telecommunication systems; LO 11 - perform analysis of connections between information processes on remote computer systems; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions; LO 15 - use modern software and hardware of information and communication technologies; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;

	LO 18 - use software and software and hardware systems for the protection of information resources; LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems; LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 3. Ability to use software and software-hardware complexes of information security in information and telecommunication (automated) systems.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions; LO 15 - use modern software and hardware of information and communication technologies; LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 18 - use software and software and hardware systems for the protection of information resources; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 29 - to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity; LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information; LO 50 - to provide) functioning of software and software-hardware complexes of detection of intrusions of different levels and classes (statistical, signature, statistical-signature); LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 4. Ability to ensure business continuity in	LO 9 - implement processes based on national and international

accordance with established information and / or cybersecurity policies.	standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 24 - to solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role); LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems; LO 29 - to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes; LO 32 - to solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy; LO 34 - to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity; LO 42 - to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards; LO 45 - apply rini classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets; LO 46 - to analyze and minimize the risks of information processing in information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis

	of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 18 - use software and software and hardware systems for the protection of information resources; LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 21 - to solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information and information and telecommunications (automated) systems; LO 22 - to solve problems of management of procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and / or cybersecurity; LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems; LO 24 - to solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role); LO 25 - to ensure the introduction of accountability management system for access to electronic information resources and processes in information and information and telecommunications (automated) systems using event logs, their analysis and established protection procedures; LO 26 - implement measures and ensure the implementation of processes to prevent unauthorized access and protection of information, information and telecommunications (automated) systems based on the reference model of interaction of open systems; LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems; LO 28 - to analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during tests in accordance with the established policy of information and / or cybersecurity; LO 29 - to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes; LO 32 - to solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy; LO 34 - to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and /

	or cybersecurity; LO 42 - to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards; LO 45 - apply rini classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets; LO 46 - to analyze and minimize the risks of information processing in information and telecommunications systems; LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information; LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems; LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems; LO 50 - to provide) functioning of software and software-hardware complexes of detection of intrusions of different levels and classes (statistical, signature, statistical-signature); LO 51 - maintain performance and ensure the configuration of intrusion detection systems in information and telecommunications systems; LO 52 - use tools for monitoring processes in information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 6. Ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyberattacks, failures and failures of various classes and origins.	LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems; LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems; LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems; LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems; LO 49 - to ensure the proper functioning of the monitoring

	system of information resources and processes in information and telecommunication systems; LO 52 - use tools for monitoring processes in information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats
PC 7. Ability to implement and ensure the functioning of complex information security systems (complexes of legal, organizational and technical means and methods, procedures, practices, etc.).	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity.
PC 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems; LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems; LO 25 - to ensure the introduction of accountability management system for access to electronic information resources and processes in information and information and telecommunications (automated) systems using event logs, their analysis and established protection procedures; LO 29 - to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes; LO 32 - to solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy; LO 34 - to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity;

	LO 42 - to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards; LO 45 - apply rini classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets; LO 46 - to analyze and minimize the risks of information processing in information and telecommunications systems; LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems; LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems; LO 50 - to provide) functioning of software and software-hardware complexes of detection of intrusions of different levels and classes (statistical, signature, statistical-signature); LO 51 - maintain performance and ensure the configuration of intrusion detection systems in information and telecommunications systems; LO 52 - use tools for monitoring processes in information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 9. Ability to carry out professional activities on the basis of the implemented information and / or cybersecurity management system.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 21 - to solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information and information and telecommunications (automated) systems; LO 24 - to solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role); LO 25 - to ensure the introduction of accountability management system for access to electronic information resources and processes in information and information and telecommunications (automated) systems using event logs, their analysis and established protection procedures; LO 28 - to analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during tests in accordance with the established policy of information and / or cybersecurity; LO 29 - to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes; LO 34 - to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to

	unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity; LO 42 - to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards; LO 45 - apply rini classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets; LO 46 - to analyze and minimize the risks of information processing in information and telecommunications systems.
PC 10. Ability to apply methods and means of cryptographic and technical protection of information at the objects of information activities.	LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems; LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information; LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.
PC 11. Ability to monitor the functioning of information, information and telecommunications (automated) systems in accordance with the established policy of information and / or cybersecurity.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 10 - perform analysis and decomposition of information and telecommunication systems; LO 11 - perform analysis of connections between information processes on remote computer systems; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions; LO 15 - use modern software and hardware of information and communication technologies; LO 18 - use software and software and hardware systems for the protection of information resources; LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems; LO 21 - to solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information

	and information and telecommunications (automated) systems; LO 22 - to solve problems of management of procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and / or cybersecurity; LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems; LO 24 - to solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role); LO 25 - to ensure the introduction of accountability management system for access to electronic information resources and processes in information and information and telecommunications (automated) systems using event logs, their analysis and established protection procedures; LO 26 - implement measures and ensure the implementation of processes to prevent unauthorized access and protection of information, information and telecommunications (automated) systems based on the reference model of interaction of open systems; LO 32 - to solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy; LO 42 - to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems; LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems; LO 50 - to provide) functioning of software and software-hardware complexes of detection of intrusions of different levels and classes (statistical, signature, statistical-signature); LO 51 - maintain performance and ensure the configuration of intrusion detection systems in information and telecommunications systems; LO 52 - use tools for monitoring processes in information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and / or cybersecurity policies.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents; LO 28 - to analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during tests in accordance with the established policy of information and / or cybersecurity;

	LO 29 - to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes; LO 34 - to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization; LO 35 - to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity; LO 42 - to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards; LO 45 - apply rini classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets; LO 46 - to analyze and minimize the risks of information processing in information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats.

Curriculum of the discipline

Content module 1. Types of cryptographic transformations of information. Modern symmetric cryptographic systems

Topic 1. Basic concepts and definitions of cryptography. History of cryptography. Principles of cryptographic protection of information.
Topic 2. Simple ciphers. Permutation codes. Replacement codes (substitutions).
Topic 3. Symmetric ciphers. Block ciphers. Streaming ciphers
Topic 4. Cryptanalysis and types of cryptanalytic attacks.
Topic 5. Modern block ciphers: 3DES, GOST 28147-2009, AES, Kalina-256.
Topic 6. Pseudo-random sequence generators.

Content module 2. Public key cryptographic systems

Topic 7. Principles of public key encryption.
Topic 8. Cryptosystem of RSA encryption. Protocols for ensuring the authenticity and confidentiality of data.
Topic 9. Diffie-Gelman cryptosystem (DH).
Topic 10. Cryptography on elliptic curves. Cryptosystem on elliptical Diffie-Gelman curves on elliptic curves (EDH)
Topic 11. Fundamentals of quantum cryptography.
Topic 12. Quantum algorithms of Shore and Grover.

The list of laboratory classes, as well as questions and tasks for independent work is given in the table "Rating-plan of the discipline".

Teaching and learning methods

In the course of teaching the discipline the teacher uses explanatory-illustrative (information-receptive) and reproductive teaching methods for topics 1, 2, and 8. Problem-based lectures, presentations, conversations, individual and group mini-projects are used as teaching methods in topics 3-7, and 9-12, that are aimed at activating and stimulating the educational and cognitive activities of applicants.

The procedure for evaluating learning outcomes

The system of assessment of formed competencies in students takes into account the types of classes, which in accordance with the curriculum of the discipline include lectures and laboratory classes, as well as independent work. Assessment of the formed competencies of students is carried out according to the accumulative 100-point system. Control measures include:

1) current control, which is carried out during the semester during lectures and laboratory classes and is estimated by the amount of points scored (maximum amount - 100 points; the minimum amount that allows a student to set off - 60 points);

2) final / semester control, which is conducted in the form of a exam, in accordance with the schedule of the educational process for 1 and 2 semesters.

The procedure for the current assessment of students' knowledge.

Assessment of student knowledge during lectures and laboratory classes is carried out according to the following criteria:

implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;

to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge, concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information streams, processes for internal and remote components;

solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role);

solve problems of data flow protection in information, information and telecommunication (automated) systems;

to assess the possibility of realization of potential threats to the information processed in information and telecommunication systems and the effectiveness of the use of complexes of means of protection in the conditions of realization of threats of different classes;

to solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy;

solve problems of ensuring the continuity of business processes of the organization on the basis of risk theory;

participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization;

to solve problems of providing and support of complex systems of information protection, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and / or cybersecurity;

implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents;

apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents;

solve problems of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards;

apply various classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets;

to analyze and minimize the risks of information processing in information and telecommunications systems;

to solve the problem of analysis of program code for the presence of possible threats.

The discipline provides the following methods of current formative assessment: interviews and oral comments of the teacher on his results, instructions of teachers in the process of laboratory tasks, the formation of self-assessment skills and discussion of completed laboratory tasks, control of individual performance.

All work must be done independently in order to develop a creative approach to solving problems.

Lectures: the maximum number of points is 12 (work on lectures - 12).

Laboratory classes: the maximum number of points is 48 (defense of laboratory works - 24, control works - 24), and the minimum - 22.

Independent work: consists of the time that the applicant spends on preparation for laboratory work and preparation for the exam in the discipline, in the technological map points for this type of work are not allocated.

Final control: is carried out taking into account the exam.

The examination ticket covers the program of the discipline and provides for the determination of the level of knowledge and the degree of mastery of competencies by students.

Each exam ticket consists of 3 practical situations (one stereotypical, one diagnostic and one heuristic task), which involve solving typical professional tasks in the workplace and allow to diagnose the level of theoretical training of the student and his level of competence in the discipline. Evaluation of each task of the examination ticket is as follows: the first task is 20 test tasks of the closed form, its performance is estimated by 20 points; the second task - devoted to the development of a structural scheme for building a corporate network of the company, its implementation is estimated at 10 points; the third task - calculation, its performance is estimated at 10 points.

The result of the semester exam is evaluated in points (maximum number - 40 points, minimum number of credits - 25 points) and is affixed in the appropriate column of the examination "Information of performance".

A student should be considered certified if the sum of points obtained from the final / semester test is equal to or exceeds 60. The minimum possible number of points for current and modular control during the semester is 35 and the minimum possible number of points scored in the exam is 25.

The final grade in the discipline is calculated taking into account the points obtained during the current control of the accumulative system. The total result in points for the semester is: "60 or more points - credited", "59 or less points - not credited" and is entered in the test "Statement of performance" of the discipline.

The final grade is set according to the scale given in the table "Assessment scale: national and ECTS".

Forms of assessment and distribution of points are given in the table "Rating-plan of the discipline".

Assessment scale: national and ECTS

The sum of points for all types of educational activities	Score ЄКТС	Score on a national scale	
		for exam, course project (work), practice	For credit
90 – 100	A	excellent	credited
82 – 89	B	fine	
74 – 81	C		
64 – 73	D	satisfactorily	

60 – 63	E		
35 – 59	FX	unsatisfactorily	Not credited

Rating plan of the discipline

Topic	Forms and types of education		Forms of evaluation	Max ball
Topic 1	***Classroom work***			
	Lecture	*Topic 1. Basic concepts and definitions of cryptography. History of cryptography. Principles of cryptographic protection of information.*	Work on lectures	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 2	***Classroom work***			
	Lecture	*Topic 2. Simple ciphers. Permutation codes. Replacement codes (substitutions).*	Work on lectures	1
	Laboratory lesson	Laboratory work № 1*"Programming hash functions"*	performing laboratory tasks	6
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 3	***Classroom work***			
	Lecture	*Topic 3. Symmetric ciphers. Block ciphers. Streaming ciphers*	Work on lectures	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 4	***Classroom work***			
	Lecture	*Topic 4. Cryptanalysis and types of cryptanalytic attacks.*	Work on lectures	1
	Laboratory lesson	Laboratory work № 2*."Building block ciphers"*	implementation laboratory work	6
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Exam preparation		

Topic 5	***Classroom work***			
	Lecture	*Topic 5. Modern block ciphers: 3DES, GOST 28147-2009, AES, Kalina-256.*	Work on lectures	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Exam preparation		
Topic 6	***Classroom work***			
	Lecture	*Topic 6. Pseudo-random sequence generators.*	Work on lectures	1
	Laboratory lesson	Laboratory work № 3.*"Perform DES encryption"*	implementation laboratory work	6
			Test work 2	6
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks.		
Topic 7	***Classroom work***			
	Lecture	*Topic 7. Principles of public key encryption.*	Work on lectures	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Exam preparation		
Topic 8	***Classroom work***			
	Lecture	*Topic 8. Cryptosystem of RSA encryption. Protocols for ensuring the authenticity and confidentiality of data.*	Work on lectures	1
	Laboratory lesson	Laboratory work № 4.*"Performing RSA encryption"*.	implementation laboratory work	6
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Exam preparation: performing typical theory tasks		
Topic 9	***Classroom work***			
	Lecture	*Topic 9. Diffie-Gelman cryptosystem (DH)*	Work on lectures	1
	Individual work			

	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Preparation for the exam: performing typical tasks on the practical component		
	Classroom work			
Topic 10	Lecture	*Topic 10. Cryptography on elliptic curves. Cryptosystem on elliptical Diffie-Gelman curves on elliptic curves (EDH)*	Work on lectures	1
	Laboratory lesson	Laboratory work № 5.*"Encryption based on elliptic curves"*	implementation laboratory work	6
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Preparation for the exam: performing typical tasks on the practical component		
Topic 11	Lecture	*Topic 11. Fundamentals of quantum cryptography.*	Work on lectures	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Preparation for the exam: performing typical tasks on the practical component		
Topic 12	Lecture	*Topic 12. Quantum algorithms of Shore and Grover.*	Work on lectures	1
	Laboratory lesson	Laboratory work № 6. *"Research of digital signature algorithm".*	implementation laboratory work	6
			Test work 2	6
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks. Preparation for the exam: performing typical tasks on the practical component		

	Examination			40

Recommended Books

Basic

1. Forouzan, Behrouz A. Introduction to cryptography and network security / Behrouz A. Forouzan. McGrawHill – 2015. – 752 p.
2. Forouzan, Behrouz A. Foundations of Computer Science, / Behrouz A. Forouzan. McGrawHill – 2018. – 715 p.

Additional

3. Forouzan, Behrouz A. Data communications and networking *I* Behrouz A Forouzan. - 4th ed. – 2017. - 1171 p. (McGraw-Hill Forouzan networking series).

Information resources.

4. www.cyberpol.ru - Computer crime and ways to fight.
5. www.iso27000.ru - Information portal dedicated to information security management.
6. www.itsec.ru - Online magazine "Information Security".
7. www.inside-zi.ru - Information and methodical magazine "Information protection. Inside.
8. www.kaspersky.ru – Laboratory of Kaspersky.
9. www.drweb.com – Laboratory DrWeb.
10. Site of personal educational systems of KhNEU named after S. Kuznets of the discipline "Theoretical foundations of cryptography"https://pns.hneu.edu.ua/course/view.php?id=5733