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

"ЗАТВЕРДЖУЮ"
Проректор
з навчально-методичної роботи
_____
Карпа ЛЕМАШКАЛО

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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 OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS

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

MANAGEMENT OF INFORMATION SECURITY

working program of the discipline

Branch of knowledge	***12 Information technologies***
Specialty	***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:
Yevseiev S.P., Doctor of technical science, Prof. of CIT Department
Goloskokova A.O., Ph.D., Assoc. 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 "Management of information security" consists of two modules. The first considers the possibility of creating effective management of information security incidents according to international standards by considering the theoretical foundations of IS management, PDCA model and stages of effective management of information security incidents according to international standards ISO 27035 and ISO 18044. The features of incident management according to the requirements of the international standard ITIL, the concept of IS incident response team (CERT / CSIRT), tools for the effective functioning of IS incident response teams are proposed for consideration.

Within the framework of the second module of the discipline the possible formulation of problems of information risk analysis and management in the organization of the information security regime in companies is considered. The international concept of information security is considered, as well as various approaches and recommendations for solving the problems of risk analysis and management. An overview of the main standards in the field of information protection and risk management: ISO 17799, ISO 15408, BSI, NIST, MITER is given. The relationship between the tasks of security analysis and intrusion detection with the task of risk management is shown. Technologies for assessing the effectiveness of information security in companies are presented.

The purpose of the discipline is to form theoretical knowledge of the basic principles of incident and risk management based on the requirements of international regulators.

The results of the study of the discipline are the acquisition of skills in the use of modern software for the evaluation, analysis and protection of information that is processed in information and communication systems from modern threats and incidents.

Characteristics of the discipline

Cource	**2**
Semester	**3**
Number of ECTS credits	**4**
Form of final control	**Credit**

Structural and logical scheme of studying the discipline

Prerequisites	Postrequisites
Information security of the state	Information systems and Internet technologies
Fundamentals of building and protecting modern operating systems	Fundamentals of mathematical modeling
Introduction to Networks	Security in information and communication systems

Competences and learning outcomes in the discipline

Competences	Learning outcomes
GC 1. Ability to apply knowledge in practical situations.	LO1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication; LO 2 - to organize own professional activity, to choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, to estimate their efficiency; 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 decisions; LO 18 - use software and hardware-software systems for 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 21 - 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 35 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 53 - 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.
GC 2. Knowledge and understanding of the subject area and understanding of the profession.	LO1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication; LO 2 - to organize own professional activity, to choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, to estimate their efficiency; 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 decisions; LO 5 - to adapt in the conditions of frequent change of technologies of professional activity, to predict the final result; LO 6 - critically comprehend the basic theories, principles, methods and concepts in teaching and professional activities; LO 7 - act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international in the field of information

	and / or cybersecurity; LO 8 - prepare proposals for regulations on information and / or cybersecurity; LO 17 - to provide processes of protection and functioning of information and 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.
GC 3. Ability to communicate professionally in state and foreign languages both orally and in writing.	LO1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
GC 4. Ability to identify, pose and solve problems in a professional direction.	LO 2 - to organize own professional activity, to choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, to estimate their efficiency; 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 decisions; LO 5 - to adapt in the conditions of frequent change of technologies of professional activity, to predict the final result; LO 7 - act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international in the field of information and / or cybersecurity; LO 8 - prepare proposals for regulations on information and / or cybersecurity; LO 53 - solve problems of analysis of program code for the presence of possible threats;
GC 5. Ability to search, process and analyze information.	LO 2 - to organize own professional activity, to choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, to estimate their efficiency; 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 decisions; LO 5 - to adapt in the conditions of frequent change of technologies of professional activity, to predict the final result; LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 28 - analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during testing in accordance with the established policy of information and / or cybersecurity;
GC 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 development, the rule of law, human and civil rights and freedoms in Ukraine.	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.
GC 7. Ability to preserve and multiply 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 in order to carry out professional activities in the field of information and / or cybersecurity.	LO 7 - act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international in the field of information and / or cybersecurity; LO 8 - prepare proposals for regulations on 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 33 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory; LO 34 - 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; LO 44 - 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 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 and 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 hardware-software systems for 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 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 - solve problems of analysis of program code for the presence of possible threats; 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 and 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 hardware-software systems for 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 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 - 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 and 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 hardware-software systems for 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; 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 ensure) the functioning of software and hardware-hardware systems for detecting intrusions of different levels and classes (statistical, signal-based, statistical-signal-based); LO 53 - solve problems of analysis of program code for the presence of possible threats;
PC 4. Ability to ensure business continuity 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 17 - to provide processes of protection and functioning of information and 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 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 33 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory; LO 34 - 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 42 - 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 - 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 46 - to analyze and minimize the risks of information processing in information and telecommunications systems; LO 53 - 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 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 and 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 hardware-software systems for 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 21 - 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 - ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information-telecommunication (automated) systems with the use of event registration logs, their analysis and established protection procedures; LO 28 - analyze and evaluate the effectiveness and level of

	protection of resources of different classes in information and information-telecommunication (automated) systems during testing 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 - 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 42 - 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 - 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 50 - to ensure) the functioning of software and hardware-hardware systems for detecting intrusions of different levels and classes (statistical, signal-based, statistical-signal-based); LO 53 - 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	LO 17 - to provide processes of protection and functioning of information and 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;

various classes and origins.	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 53 - solve problems of analysis of program code for the presence of possible threats;
PC 7. Ability to implement and ensure the functioning of integrated information security systems (complexes of legal, organizational and technical means and methods, procedures, techniques, 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy;
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 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 25 - ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information-telecommunication (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 33 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory; LO 34 - 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 - solve problems of providing and maintaining complex information protection systems, as well as

	counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 42 - 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 - 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 50 - to ensure) the functioning of software and software-hardware systems for detecting intrusions of different levels and classes (statistical, signature, statistical-signature); LO 53 - 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 - 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 - ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information-telecommunication (automated) systems with the use of event registration logs, their analysis and established protection procedures; LO 28 - analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during testing 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 33 - to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory; LO 34 - 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 42 - 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 - 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 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;
PC 11. Ability to monitor the functioning of information, information and telecommunication (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 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 hardware-software systems for protection of information resources; LO 21 - 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 - ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information-telecommunication (automated) systems using event logs, their analysis and established protection procedures; LO 42 - 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 50 - to ensure) the functioning of software and software-hardware systems for detecting intrusions of different levels and classes (statistical, signature, statistical-signature); LO 53 - 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 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 - analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during testing 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 33 - to solve the problem of ensuring the continuity of

	business processes of the organization on the basis of risk theory; LO 34 - 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 - solve problems of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy; LO 42 - 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 - 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 - solve problems of analysis of program code for the presence of possible threats;

Curriculum of the discipline

Content module 1. Effective management of the information security incidents according to the international standards requirements.

Theme 1. Theoretical fundamentals of the information security management.

Theme 2. PDCA model of the information security incidents management processes life cycle description. Stages of the effective management of the information security incidents according to the requirements of the international standards ISO 27035 and ISO 18044 7.

Theme 3. Features of the incident management according to the requirements of the international standard ITIL.

Theme 4. The concept of the information security incidents response team (CERT / CSIRT): development history and possible benefits for the entrepreneurship. Generalized classification of CERT / CSIRT groups: scope of activity, goals and potential clients

Theme 5. Basic stages of creation of CERT / CSIRT groups: from habitat environment identification to cooperation at the international level.

Theme 6. Tools for the effective functioning of the response teams to the information security incidents.

Content module 2. Information security risk management.

Theme 7. Risk analysis in the information security environment.

Theme 8. Risk management and the international standards.

Theme 9. Risk analysis technologies.

Theme 10. Risk analysis tools.

Theme 11. Security audit and risk analysis.
Theme 12. Detection of attacks and risk management.

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. Lectures (1-12), presentations (1-12) are used as teaching methods 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 test, in accordance with the schedule of the educational process.

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:

- ability to implement processes based on standards, detection, identification, analysis and response to cybersecurity incidents;
- the ability to assess the feasibility of threats in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats;
- ability to analyze and evaluate the effectiveness and level of protection of resources of different classes in the systems during the tests in accordance with the established cybersecurity policy;
- ability to apply national and international cybersecurity regulations to investigate incidents;
- ability to analyze and minimize the risks of information processing in information and telecommunications systems.

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.

Final control of knowledge and competencies of students in the discipline is carried out on the basis of accumulated points for completed current and control tasks in lectures and laboratory classes, which reflects the student's understanding of the program as a whole, logic and relationships between individual sections, ability to creatively use accumulated knowledge. the ability to formulate their attitude to a particular problem of the discipline, etc.

Lecture classes: the maximum number of points is 42 (lecture work – 12, module tests – 30)

Practical (seminar, laboratory) classes: the maximum number of points is 58, and the minimum – 24 (working at laboratory works).

Independent work: consists of the time that the student spends on preparation for laboratory work and on the preparation of their defense and performance of tests in the discipline, in the technological map points for this type of work are not allocated.

Final control: is carried out on the accumulated points.

A student should be considered certified if the sum of points obtained as a result of the final / semester performance test is equal to or exceeds 60. The final grade in the discipline is calculated taking into account the points obtained during the test and points obtained during the current control of the accumulation 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 success" of the discipline.

The final grade is set according to the scale given in the table "Grade 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
3rd semester

Topic	Forms and types of education		Forms of evaluation	Max points
Topic 1	***Classroom work***			
	Lecture	*Lecture "Theoretical fundamentals of the information security management"*	Lecture	1
	Laboratory lesson	*Laboratory work 1. Deployment of an operating system for audit of the computer networks and systems information security*	Laboratory lesson	2
	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	*Lecture "PDCA model of the information security incidents management processes life cycle description. Stages of the effective*	Lecture	1

		management of the information security incidents according to the requirements of the international standards ISO 27035 and ISO 18044 7”		
	Laboratory lesson	*Laboratory work 2. Tools for covert collection of technical information from a computer system or network.*	Laboratory lesson	2
	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	*Lecture "Features of the incident management according to the requirements of the international standard ITIL"*	Lecture	1
	Laboratory lesson	*Laboratory work 2. Tools for covert collection of technical information from a computer system or network.*	Laboratory lesson	2
			Answer of laboratory work 1, 2	4
	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	*Lecture " The concept of the information security incidents response team (CERT / CSIRT): development history and possible benefits for the entrepreneurship. Generalized classification of CERT / CSIRT groups: scope of activity, goals and potential clients"*	Lecture	1
	Laboratory lesson	*Laboratory work 3. Investigation of system or network vulnerabilities using a specialized vulnerability scanner - Nessus*	Laboratory lesson	2
	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 5	***Classroom work***			
	Lecture	*Lecure "Basic stages of creation of CERT / CSIRT groups: from habitat environment identification to cooperation at the international level."*	Lecture	1
	Laboratory lesson	*Laboratory work 3. Investigation of system or network vulnerabilities using a specialized vulnerability scanner - Nessus*	Laboratory lesson	2
			Answer of laboratory work 3	5
	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 test		
Topic 6	***Classroom work***			
	Lecture	*Lecure "Tools for the effective functioning of the response teams to the information security incidents"*	Lecture	1
	Laboratory lesson	*Laboratory work 4. Search of the vulnerabilities and sensory information in open resources with Maltego*	Laboratory lesson	2
			Answer of laboratory work 3	5
			Module test 1	15
	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	*Lecture "Risk analysis in the information security "*	Lecture	1
	Laboratory lesson	*Laboratory work5. Collection of the technical and sensory information using sniffers software*	Laboratory lesson	2
	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 8	***Classroom work***			
	Lecture	*Lecture "Risk management and the international standards."*	Lecture	1
	Laboratory lesson	*Laboratory work 5. Collection of the technical and sensory information using sniffers software*	Laboratory lesson	2
			Answer of laboratory work 5	5

	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 9	***Classroom work***			
	Lecture	*Lecture "Risk management and the international standards."*	Lecture	1
	Laboratory lesson	*Laboratory work 5. Collection of the technical and sensory information using sniffers software*	Laboratory lesson	2
			Answer of laboratory work 5	5
	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 10	***Classroom work***			
	Lecture	*Lecture "Risk analysis tools."*	Lecture	1
	Laboratory lesson	*Laboratory work 6. Snifers*	Laboratory lesson	2
			Answer of laboratory work 5	5
	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 test	.	
Topic 11	***Classroom work***			
	Lecture	*Lecture " Security audit and risk analysis."*	Lecture	1
	Laboratory lesson	*Laboratory work 7. A tool for study the vulnerabilities of wireless Wi-Fi networks – Aircrack*	Laboratory lesson	2
			Module test 2	15

	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 12	***Classroom work***			
	Lecture	*Lecture " Detection of attacks and risk management."*	Lecture	1
	Laboratory lesson	*Laboratory work 7. A tool for study the vulnerabilities of wireless Wi-Fi networks - Aircrack*	Laboratory lesson	2
			Answer of laboratory work 7	5
	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		

Recommended Books

Basic

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf .

Additional

2. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

3. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. Доступно: zakon.rada.gov.ua/laws/show/v0365500-11.

4. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

5. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. Доступно: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii. Дата звернення: Груд. 7.2017.

6. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11425.

7. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005

8. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

Information resources.

9. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Менеджмент інформаційної безпеки” https://pns.hneu.edu.ua/course/view.php?id=4924.