МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

БЕЗПЕКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

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 *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Долгова Н.Г., к.т.н., доц. кафедри КІТ,

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMIC

"APPROVED"
Vice-rector for educational and methodical work

Karina NEMASHKALO

SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS

working program of the educational discipline

Field of knowledge	**12 "INFORMATION TECHNOLOGIES"**
Specialty	**125 "CYBER SECURITY"**
Educational level	**first (bachelor's)**
Educational program	**CYBER SECURITY**

Discipline status	mandatory
Teaching language	English

Head of the *Department of cyber security and information technologies* — *Olha STARKOVA*

Kharkiv
2022

APPROVED
at a meeting of the Department of Cybersecurity and Information Technology
Protocol № 1 dated August 27, 2022

Developers:
Dolgova N.G., Ph.D., Assoc. Prof. of the Department of KIT

Update and re-approval letter
working program of the discipline

Academic year	Date of the meeting of the department- developer of WPD	Protocol number	gnature of the head of the department

Introduction

Summary of the discipline:

Discipline "Security in information and communication systems" consists of two

modules, the first considers modern threats to network security, the concept of ensuring the security of network devices, the introduction of firewall technologies, the introduction of an intrusion prevention system.

The second module of the discipline considers the issues of local area network (LAN) security, cryptographic systems, the introduction of virtual private networks (VPN), the introduction of a multifunctional security device Cisco Adaptive Security Appliance (ASA).

Characteristics of the discipline

Course	**3**
Semester	**6**
Number of ECTS credits	**5**
Final control form	exam

Structural and logical scheme of studying the discipline

Prerequisites	Post requisites
Introduction to networks	Information systems and Internet technologies
Mathematical foundations of cryptology	Fundamentals of technical protection of information
Basics of construction and protection of modern operating systems	Basics of cryptographic protection

Competencies and learning outcomes in the discipline

Competencies	Learning outcomes
CG 1. Ability to apply knowledge in practical situations. CG 2. Knowledge and understanding of the subject area and understanding of the profession. CG 3. Ability to communicate professionally in the state and foreign languages both orally and in writing.	LO 1 - apply knowledge of state and foreign languages to ensure the effectiveness of professional communication;
CG 1. Ability to apply knowledge in practical situations. CG2. Knowledge and understanding of the subject area and understanding of the profession.	LO 2 - organize own professional activity, choose optimal methods and ways to solve complex specialized tasks

CG 4. Ability to identify, formulate and solve problems in the professional field. CG 5. Ability to search, process and analyze information	and practical problems in professional activity, 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 tasks and practical problems in professional activities characterized by complexity and incomplete certainty of conditions, and be responsible for the decisions made;
CG 2. Knowledge and understanding of the subject area and understanding of the profession. CG 4. Ability to identify, formulate and solve problems in the professional field. CG 5. Ability to search, process and analyze information	LO 5 - to adapt to the conditions of frequent changes in the technologies of professional activity, to predict the final result;
CG 2. Knowledge and understanding of the subject area and understanding of the profession.	LO 6 - critically comprehend the basic theories, principles, methods and concepts in learning and professional activities;
CG 2. Knowledge and understanding of the subject area and understanding of the profession. CG 4. Ability to identify, formulate and solve problems in the professional field. PC 1. Ability to apply the legislative 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 ones in the field of information and/or cybersecurity;

CG 5. Ability to search, process and analyze information. CS 1. Ability to apply the legislative 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. CS 2. Ability to use information and communication technologies, modern methods and	LO 9 - implement processes based on national and international standards for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents;

models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origins. CS 7. Ability to implement and ensure the functioning of integrated information security systems (complexes of regulatory, organizational and technical means and methods, procedures, practices, etc.) CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	
CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity.	LO 10 - to analyze and decompose information and telecommunication systems;

CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy	
CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 11 - analyze the relationship between information processes on remote computer systems;
CS 7. Ability to implement and ensure the functioning of integrated information security systems (complexes of regulatory, organizational and technical means and methods, procedures, practices, etc.) CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	PH 12 - develop threat and offender models

CG 5. Ability to search, process and analyze information. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. .CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information	LO 13 - analyze the design of information and telecommunication systems based on standardized technologies and data transfer protocols;

resources in accordance with the established information and/or cybersecurity policy	
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 14 - to solve the problem of protecting programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions made;
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 15 - use modern software and hardware of information and communication technologies;

CG 2. Knowledge and understanding of the subject area and understanding of the profession. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity.	LO 17 - to ensure the processes of protection and operation of information and telecommunication (automated) systems based on practices, skills and knowledge of structural (structural and logical) schemes, network topology, modern architectures and models of

CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 10. Ability to apply methods and means of cryptographic and technical protection o f information at the objects of information activity. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	protection of electronic information resources with the reflection of interconnections and information flows, processes for internal and remote components;

CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 18 - use software and hardware and software systems to protect information resources;

CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 19 - apply theories and methods of protection to ensure the security of information in information and telecommunication systems;

CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origins. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities.	LO 20 - to ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems;

CG 1. Ability to apply knowledge in practical situations. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	TLO 21 - to solve the tasks of ensuring and maintaining (including: review, testing, accountability) the access control system in accordance with the established security policy in information and information and telecommunication (automated) systems;
CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 23 - to implement measures to counteract unauthorized access to information resources and processes in information and information and telecommunication (automated) systems
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system.	LO 24 - to solve problems of access control to information resources and processes in information and information and telecommunication (automated) systems based on access control models (mandatory, discretionary, role-based);

CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 25 - to ensure the introduction of accountability of the system for managing access to electronic information resources and processes in information and information and telecommunication (automated) systems using event logs, their analysis and established security procedures;
CG 1. Ability to apply knowledge in practical situations. formations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin.	LO 27 - to solve problems of data flow prection in information, information and telecommunication (automated) systems;

CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to	LO 28 To analyze and evaluate the effectiveness and level of security of resources of different classes in information and information and telecommunication (automated) systems during tests in accordance with the established information and/or cybersecurity policy;

implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin.	
CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 29 - to assess the possibility of potential threats to information processed in information and telecommunication systems and the effectiveness of the use of security systems in the face of threats of various classes;
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 10. Ability to apply methods and means of cryptographic and technical protection o f information at information activities.	LO 31 - to apply theories and methods of protection to ensure the security of elements of information and telecommunication systems;
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy.	LO 32 - to solve the tasks of managing the processes of restoring the normal functioning of information and telecommunication systems using backup procedures in accordance with the established security policy;

CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CG 1. Ability to apply the legislative 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. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 33 - to solve the problems of ensuring the continuity of the organization's business processes based on risk theory;

CG 1. Ability to apply the legislative 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. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing	LO 34 To participate in the development and implementation of the information security and/or cybersecurity strategy in accordance with the goals and objectives of the organization;

factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	
CG 1. Ability to apply knowledge in practical situations. CS 1. Ability to apply the legislative 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. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 7. Ability to implement and ensure the functioning of integrated information security systems (complexes of regulatory, organizational and technical means and methods, procedures, practices, etc.) CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 35 - to solve the tasks of providing and maintaining integrated information security systems, as well as counteracting unauthorized access to information resources and processes in information and information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy;

CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origins. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system.	LO 37 - to measure the parameters of dangerous and interfering signals during instrumental control of information security processes and determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system;

CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origins. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities.	LO 38 - interpret the results of special measurements using technical means, control of information and telecommunication systems characteristics in accordance with the requirements of regulatory documents of the technical information security system
CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 42 - implement processes for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents;

LO 2. Knowledge and understanding of the subject area and understanding of the profession. PC 1. Ability to apply the legislative 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. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement 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;

CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CG 1. Ability to apply the legislative 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. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 44 - to solve the problems of ensuring the continuity of the organization's business processes based on the risk theory and the established information security management system, in accordance with national and international requirements and standards;

CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them.	LO 45 - apply different classes of information security and/or cybersecurity policies based on risk-based access control to information assets;

CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 46 To analyze and minimize the risks of information processing in information and telecommunication systems;
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at the objects of information activity.	LO 47 - to solve the problems of protecting information processed in information and telecommunication systems using modern methods and means of cryptographic information protection;

CS 5. Ability to ensure the protection of information processed in information and	LO 48 - to implement and maintain intrusion detection systems and use

telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	cryptographic security components to ensure the required level of information security in information and telecommunications systems;
CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 49 - to ensure proper functioning of the system for monitoring information resources and processes in information and telecommunication systems;

CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them.	LO 52 - use tools to monitor processes in information and telecommunication systems;

CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CG 1. Ability to apply knowledge in practical situations. CG 4. Ability to identify, formulate and solve problems in the professional field. CG 5. Ability to search, process and analyze information. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 53 To solve problems of analyzing program code for possible threats;

CG 1. Ability to apply knowledge in practical situations. CG 2. Knowledge and understanding of the subject area and understanding of the profession.	LO 54 - to realize the values of civil (free democratic) society and the need for its sustainable development, the rule of

CG 6. Ability to exercise one's 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. CG 7. Ability to preserve and increase moral, cultural, scientific values and achievements of society based on an understanding of 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, technology and technology, to use various types and forms of physical activity for active recreation and healthy lifestyle	law, human and civil rights and freedoms in Ukraine

Program of the discipline

Content module 1: Network security applications

Topic 1: Modern threats to network security
Topic 2. Ensuring the security of network
devices
Topic 3: Authentication, authorization, and accounting
Topic 4. Implementation of firewall technologies
Topic 5. Implementation of an intrusion prevention system

Content module 2. Network security

Topic 6. Securing a local area network (LAN)
Topic 7. Cryptographic systems
Topic 8: Implementing virtual private networks (VPNs)
Topic 9: Implementing the Cisco Adaptive Security Appliance (ASA) Multifunctional Security Appliance
Topic 10. Introduction to ASDM
Topic 11. Managing a secure network

The list of laboratory classes, as well as questions and assignments 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 and illustrative (information and receptive) and reproductive teaching methods. Lectures, presentations,

conversations, individual and group mini-projects are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of students.

Teaching the discipline involves the use of explanatory and illustrative (topics 1-11), reproductive (topics 3,4,5,6,8), research methods (topics 9,10), and problem-based learning methods (topic 11). Thus, during lectures, the teacher provides students with a certain amount of theoretical material, with explanations in graphic form (diagrams, tables, presentations) and with examples of problem solving. During laboratory classes, students have the opportunity to gain practical skills in solving problems based on the problem formulated on the subject of the class. Practical skills are improved during individual assignments and independent work.

These teaching methods are aimed at developing students' ability to solve complex problems in the field of web application development.

The procedure for assessing learning outcomes

The program of the discipline includes lectures, laboratory and independent work. The knowledge and competencies acquired by students during lectures are assessed by writing quizzes and taking tests, and the skills acquired during laboratory classes are assessed by solving problems related to the subject matter of the classes. Independent work is not assessed separately, as it is a preparation for other types of classes and is an integral part of education. The assessment of the formed competencies of applicants is carried out according to a cumulative 100-point rating system. Control measures include

- current control, which is carried out during the semester during lectures and laboratory classes and is evaluated by the number of points scored (maximum amount - 60 points; minimum amount of admission to the exam - 35 points)
- module control involves completion of final control tasks, which may include a creative research component and require knowledge and skills acquired during the study of a set of material on the module topic.

During the current control, students' knowledge is assessed according to the following criteria

- fluency in the full scope of the training material, with an understanding of the examples and the ability to provide their own examples to explain the essence of the material;
- demonstration of skills in applying methods of building mathematical models to solve applied problems;
- demonstration of skills in applying innovative methods of work in solving problems;
- Demonstration of skills in searching and analyzing information sources, justifying the results obtained, and drawing conclusions in the work;
- demonstration of teamwork skills in solving complex problems in the development and analysis of mathematical models.

The formation of tasks and control over their implementation are aimed at helping students acquire active creative thinking skills, instilling cognitive skills and norms of fair cooperation. The main requirement for completing assignments is to complete them independently or to determine the percentage of contribution in teamwork.

The distribution of points in the current assessment by type of work is as follows.

Lecture classes: the level of mastery of theoretical knowledge is determined during lectures, writing quizzes and tests (maximum number of points is 20).

Laboratory classes: the level of acquired skills in applying knowledge to solve problems is determined by the correctness of the tasks of laboratory work (the maximum number of points is 40).

Independent work: the level of mastery of the skills of using the latest knowledge,

methodology and methods of conducting scientific research is determined by the degree of preparation of the graduate student for laboratory work and writing tests (the technological map does not provide additional points for this type of work).

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

The exam paper covers the program of the discipline and provides for determining the level of knowledge and the degree of competence of students. Each examination paper consists of 2 theoretical questions and 1 practical task, which involve solving typical professional tasks of a specialist in the workplace and allow to diagnose the level of theoretical training of the student and the level of his/her competence in the discipline. The assessment of each task of the examination paper is as follows: the first theoretical question is worth 10 points; the second question is worth 10 points; the third practical task is a calculation task, its completion is worth 20 points.

The result of the semester exam is evaluated in points (maximum number of points - 40 points, minimum number of points - 25 points) and is put in the appropriate column of the exam "Record of academic performance". An applicant should be considered certified if the sum of points obtained as a result of the final/semester academic performance test is equal to or exceeds The minimum possible number of points for the current and module 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 exam and the points obtained during the current control under the cumulative system. The total result in points for the semester is: "60 and more points - passed", "59 and less points - failed" and is entered into the academic record of the discipline.

The forms of evaluation and distribution of points are shown in the table "Rating plan of the discipline".

Rating plan of the discipline

Topic	**Forms and types of education**		**Forms of evaluation**	**Max ball**
Topic 1.	***Classroom work***			
	Lecture	Lecture №1. Modern threats to network security.	Work in the lecture	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 2.	***Classroom work***			
	Lecture	Lecture №2. Ensuring the security of network devices.	Work in the lecture	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Top	***Classroom work***			
	Lecture	Lecture №3. Authentication, authorization and accounting.		

ic 3				
	Laboratory lesson	Laboratory work 1: Social engineering. Study of network attacks, as well as tools for security audits and attacks.	perform and defense of the laboratory work	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 4.	***Classroom work***			
	Lecture	Lecture №4. Implementation of firewall technologies.	Work in the lecture	
	Laboratory lesson	Laboratory work 2. Protecting the router for administrative access		
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 5.	***Classroom work***			
	Lecture	Lecture №5. Implementation of intrusion prevention system.	Work in the lecture	
	Laboratory lesson	Laboratory work 2. Protecting the router for administrative access.	perform and defense of the laboratory work	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Modular control	Control work		10
Topic 6.	***Classroom work***			
	Lecture	Lecture №6. Ensuring the security of the local area network (LAN).	Work in the lecture	
	Laboratory lesson	Laboratory work 3. Protecting administrative access using AAA and RADIUS.		
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		

Topic 7.	***Classroom work***			
	Lecture	Lecture №7. Cryptographic systems of information protection.	Work in the lecture	
	Laboratory lesson	Laboratory work 3. Protecting administrative access using AAA and RADIUS.	perform and defense of the laboratory work	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 8.	***Classroom work***			
	Lecture	Lecture №8. Implementation of virtual private networks (VPN).	Work in the lecture	
	Laboratory lesson	Laboratory work 4. Configuring zonal firewalls.		
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 9.	***Classroom work***			
	Lecture	Lecture №9. Implementation of a multifunctional security device Cisco Adaptive Security Appliance (ASA).	Work in the lecture	
	Laboratory lesson	Laboratory work 4. Configuring zonal firewalls.	perform and defense of the laboratory work	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 10	***Classroom work***			
	Lecture	Lecture №10 "Introduction to ASDM."	Work in the lecture	
	Laboratory lesson	Laboratory work 5. Configuring the intrusion prevention system (IPS).		
	Individual work			

.	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 11.	***Classroom work***			
	Lecture	Lecture №11. Managing a secure network.	Work in the lecture	
	Laboratory lesson	Laboratory work 5. Configuring the intrusion prevention system (IPS).	perform and defense of the laboratory work	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Modular control	Control work		10
	exam			40

Recommended literature

Basic

1. Cybersecurity: modern protection technologies. Textbook for higher education institutions. / Ostapov SE, Yevseev SP, Korol OG - Lviv: "Novyi Svit-2000", 2019. - 678 p.
2. Technologies of information protection in information and telecommunication systems [Electronic resource] : textbook / A. Zhylin, O. Shapoval, O. Uspensky. Kyiv : Igor Sikorsky Kyiv Polytechnic Institute, 2021. 213 p.
3. Information security of the state: a textbook / V. Rudnytskyi, S. Hnatiuk, N. Lada, R. Breus. - Kharkiv: DISA PLUS LLC, 2018. 359 p.
4. LAW OF UKRAINE ON PROTECTION OF INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

Additional

5. CCNA 200-301 Official Cert Guide Library By Wendell Odom, Published Dec 31, 2019 by Cisco Press. Part of the Official Cert Guide series https://issuhub.com/view/index/33465

Information resources

5. EVE - a virtual environment in the field of networking, security and DevOps https://www.eve-ng.net/
6. Website of personal learning systems of KhNUE named after S. Kuznets of the discipline "Security Engineering of Information and Communication Systems"
https://pns.hneu.edu.ua/course/view.php?id=8951