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

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи
_____ Каріна НЕМАШКАЛО

ІНЖЕНЕРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**всі**
Спеціальність	**всі**
Освітній рівень	**другий (магістерський)**
Освітня програма	**всі**

Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**англійська**

Розробник:
к.т.н., доц. підписано КЕП _____ Наталія ДОЛГОВА

Завідувач кафедри
кібербезпеки та
інформаційних технологій
д.т.н., проф. _____ Ольга СТАРКОВА

Харків
2023

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

APPROVED
at the meeting of the department
of cybersecurity and
information technologies
Protocol № 2 of 31.08.2023.

AGREED
Vice-rector for educational and methodical work
_____ Karina NEMASHKALO

SECURITY ENGINEERING OF INFORMATION AND COMMUNICATION SYSTEMS

Program of the course

Field of knowledge	**All**
Speciality	**All**
Study cycle	**second (magister's)**
Study programme	**All**

Course status	**elective**
Language	**English**

Developer:
PhD (Engineering),
Associate Professor digital signature _____ Natalya DOLGOVA

Head of Cybersecurity and
Information Technology
Department _____ Olga STARKOVA

Kharkiv
2023

INTRODUCTION

The relevance of the academic discipline and its necessity and role in the training of specialists lies in its focus on modern effective technical and organizational measures to protect confidential information and information and communication systems from malicious attacks, the application of which makes it possible to solve the tasks of cyber security of networks.

The purpose of the educational discipline "Security Engineering of Information and Communication Systems" is to teach students of higher education the principles of building complex information protection systems for the formation of the security contour of business processes in information and communication systems based on Internet technologies and applications.

The tasks of the educational discipline are: acquisition of skills in the analysis of potential threats to information security and methods of their detection, assessment and management of effective protection of information and information systems in the modern digital environment, penetration testing, recovery after incidents, processing of security events and response to incidents.

The subject of the academic discipline is the security of information and communication systems.

The object of study of the discipline is technical means, software products, processes and methods used to ensure information security in systems, as well as internal and external threats.

The learning outcomes and competencies formed by the course are defined in table 1.

Table 1

Learning outcomes and competencies formed by the course

Learning outcomes	**Competencies**
To organize one's own professional activity, to choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, to evaluate their effectiveness;	Ability to apply knowledge in practical situations. Knowledge and understanding of the subject area and understanding of the profession. The ability to identify, pose and solve problems in a professional direction. Ability to search, process and analyze information.
Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including inteRSational ones in the field of information and/or cyber security.	Knowledge and understanding of the subject area and understanding of the profession. The ability to identify, pose and solve problems in a professional direction. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security.
Perform analysis and decomposition of information and telecommunication systems.	Ability to search, process and analyze information Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. Ability to use information and communication technologies,

	modern methods and models of information security and/or cyber security. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.). Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. Ability to perform professional activities based on the implemented information and/or cyber security management system. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.
Develop threat and offender models.	Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.). The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.
Solve the task of protecting programs and information processed in information and telecommunication systems by means of Software and hardware and give an assessment of the effectiveness of the quality of the decisions made.	Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity. Ability to monitor the functioning of information, information and telecommunication (automated) systems in

	accordance with the established policy of information and/or cyber security.
Use modeRS software and hardware of information and communication technologies.	Ability to apply knowledge in practical situations. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
Solve problems of data flow protection in information, information and telecommunication (automated) systems.	Ability to apply knowledge in practical situations. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins.
To analyze and evaluate the effectiveness and level of security of resources of various classes in information and information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.	Ability to apply knowledge in practical situations. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins.
To solve the problems of ensuring the continuity of the organization's business processes on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards;	Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. Ability to perform professional activities based on the implemented information and/or cyber security management system. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.

COURSE CONTENT

Content Module 1. Network security applications

Topic 1. Modern threats to network security

1.1. Classes of networks

Class A/B/C/D/E IP addresses and network ID, host ID.

1.2. Network protection

Concepts of network security. Principles of the security system. Key elements of secure network services

1.3. Areas of network security

Multi-level protection: router protection, workstation protection, and individual device protection.

1.4. Cisco Security Architecture

Cisco Security Manager (CSM); monitoring, analysis and response system of Cisco Security (MARS); software and hardware solution for centralized access control Cisco Secure Access Control Server (ACS); Cisco IP Solution Center (ISC) platform for centralized network infrastructure management.

Topic 2. Ensuring the security of network devices

2.1. Edge router protection

Border Gateway Protocol (BGP). Common ports used for BGP. Tools for using BGP. BGP Weaknesses and Vulnerabilities.

2.2. Assignment of administrative roles

User objects and their access attributes. Procedure for creating and destroying user objects of the corresponding type.

2.3. Management and reporting protection

Confidentiality of the exchange. Functional security services "Registration", "Identification and authentication", etc.

2.4. Use of automatic security functions

Protection with Windows Security.Topic 3. Authentication, authorization and accounting

3.1. AAA review

Authentication without AAA. AAA components (authentication, authorization, audit). Authentication modes. Authorization. Audit

3.2. Configuring Local AAA Authentication Using the Command Line Interface (CLI)

Authentication of administrative access. RADIUS. TACACS +. The main differences between RADIUS and TACACS+. Authentication methods. Standard and named methods. Fine-tune your authentication configuration.

3.3. Features of AAA server authentication

Comparison of AAA local and server authentication. Familiarity with the Cisco secure access management system (Access Control System, ACS). AAA server communication protocols

3.4. Configuring AAA Server Authentication Using the Command Line Interface (CLI)

Procedure for configuring AAA server authentication using the command

line interface (CLI). Configuring the use of TACACS+ servers through the CLI. Configuring the use of RADIUS servers through the CLI. Configuring authentication using the AAA server.

Topic 4. Implementation of firewall technologies

4.1. Access control list.

Configuring standard and extended IPv4 ACLs using the command line interface (CLI). Brief information about access control lists. Configuring numbered and named ACLs. ACL application. Editing existing ACLs. Protection against spoofing using ACL lists. Passing the necessary traffic through the firewall. Prevention of malicious use of the ICMP protocol. Neutralization of SNMP exploits. Introduction to IPv6 ACLs

4.2. Technology between the network screen.

Protecting networks with a firewall. Defining a firewall. Advantages and limitations of firewalls. Description of the types of firewalls. Advantages and limitations of a packet filtering firewall. Stateful firewalls. Internet screens of a new generation.

4.3. Zonal firewalls.

Zonal Firewall (ZPF) Overview. Advantages of ZPF. Design by ZPF. Principles of ZPF operation. Actions of ZPF. ZPF configuration. Checking the ZPF configuration.

Topic 5. Implementation of the intrusion prevention system

5.1. IPS technologies.

Characteristics of IDS and IPS systems. IPS network implementations. Cisco Switched Port Analyzer. Cisco SPAN configuration using intrusion detection system.

5.2. IPS signatures.

Characteristics of IPS signatures. IPS signature alarms. IPS signature actions. Management and monitoring of IPS. IPS Global Correlation

5.3. Implementation of IPS.

Configuring Cisco IOS IPS using the Command Line Interface (CLI). Changing Cisco IOS IPS signatures. IPS testing and monitoring.

Content module 2. Network security

Topic 6. Ensuring the security of the local network (LAN)

6.1. Security of end devices.

Familiarity with end device security. Protection against malicious software. Email and web traffic protection. Network access control.

6.2. Level 2 security factors

Level 2 security threats. Attacks on CAM tables. Neutralization of the attack on the CAM table. Neutralization of attacks on VLANs. Neutralization of DHCP attacks. Neutralization of ARP attacks. Neutralization of address spoofing attacks. Spanning tree protocol. Neutralization of STP attacks.

Topic 7. Cryptographic systems.

7.1. Secure communications.

Authentication, Integrity and Privacy. Compilation of ciphertext. Permutation ciphers. Substitution codes. One-Time Pad ciphers. Cracking the code.

7.2. Cryptology.

Creating and breaking secret codes. Cryptoanalysis.

7.3. Cryptographic hashes.

Cryptographic hash function. Properties of the cryptographic hash function. Known hash functions. Ensuring integrity using MD5, SHA-1 and SHA-2 algorithms. Authentication using the HMAC algorithm. Key management. Characteristics of key management. Length in the key space. Types of cryptographic keys.

7.4. Encryption.

Two classes of encryption algorithms. Symmetric and asymmetric encryption. Symmetric block and stream encryption. Choosing an encryption algorithm. Data Encryption Standard (DES). Using 3DES. An overview of the AES standard. Alternative encryption algorithms. Diffie-Hellman key exchange.

7.5. Public key cryptography.

Comparison of symmetric and asymmetric encryption. Algorithms of asymmetric keys. Digital signatures. Public Key Infrastructure (PKI). Certification centers. Compatibility of different PKI providers. Public key cryptography standards. PKI topologies. Digital certificates and SA.

Topic 8. Implementation of virtual private networks (VPN).

8.1. Overview of VPN networks.

Introduction to VPN networks. Layer 3 IPsec VPNs. VPN technologies. Two types of VPN networks. Components of VPN networks for remote access. Components of VPN networks between two points.

8.2. Introduction to the IPsec protocol.

IPsec technologies. IPsec protocols. Internet Key Exchange.

8.3. IPsec VPN configuration between two points (Site-to-Site)

Establishing an IPsec connection. Site-to-Site IPsec VPN topology. ISAKMP policy. IPsec policy. Crypto card. IPsec VPN.

Topic 9. Implementation of the multifunctional protection device Cisco Adaptive Security Appliance (ASA)

9.1. ASA decision

ASA firewall models. Extending the functionality of the ASA firewall. Overview of firewalls in network design. Modes of operation of ASA firewalls. ASA Licensing Requirements.

9.2. Configuration between the ASA network screen

Basic ASA configuration. ASA security levels. ASA 5505 deployment scenarios. Getting to know basic ASA settings. Setting up services and management parameters. Groups of objects. ACLS. NAT services on the ASA. Service policies at ASA.

Topic 10. Introduction to ASDM

10.1. Introduction to ASDM

Preparation for work with ASDM. Starting ASDM. ASDM home page dashboards. ASDM page elements. ASDM Configuration and Monitoring Sections. ASDM wizards menu. Setting up services and management parameters. Configuring advanced ASDM features.

10.2. Site-to-Site VPN

ASA Device Support Site-to-Site VPN. VPN remote access (Remote-Access). Comparison of IPsec and SSL. Cisco AnyConnect Secure Mobility Client. Clientless SSL VPN configuration. SSL VPN configuration using the AnyConnect client.

Topic 11. Management of a secure network

11.1. Network security testing techniques

Network security testing and evaluation. Types of network tests. Network security testing tools.

11.2. Security Policy Overview

Life cycle of network security. Security policy. Security policy audience. Structure of the security policy. Standards, instructions and procedures. Roles and responsibilities. Responding to a security breach.

The list of laboratory studies in the course is given in table 2.

Table 2

The list of laboratory studies

Topic name and task name	Content
Topic 1, 2.Laboratory work 1.	Social engineering. Study of network attacks, as well as tools for security auditing and conducting attacks.
Topic 3, 4. Laboratory work 2.	Protecting the router for administrative access.
Topic 5, 6. Laboratory work 3.	Protecting administrative access using AAA and RADIUS.
Topic 7, 8. Laboratory work 4.	Setting up zonal firewalls.
Topic 9-11. Laboratory work 5.	Intrusion Prevention System (IPS) settings.

The list of self-studies in the course is given in table 3.

Table 3

List of self-studies

Topic name and task name	Content
Topic 1. Task 1	Modern threats to network security.
Topic 2. Task 2	Ensuring the security of network devices.
Topic 3. Task 3	Authentication, authorization and accounting.
Topic 4. Task 4	Implementation of firewall technologies.
Topic 5. Task 5	Implementation of the intrusion prevention system.
Topic 6. Task 6	Ensuring local area network (LAN) security.
Topic 7. Task 7	Cryptographic information protection systems.
Topic 8. Task 8	Implementation of virtual private networks (VPN).
Topic 9. Task 9	Implementation of the multifunctional protection

	device Cisco Adaptive Security Appliance (ASA).
Topic 10. Task 10	Introduction to ASDM.
Topic 11. Task 11	Secure network management.

The number of hours of lecture and laboratory classes and hours of self-study is given in the technological card of the course.

TEACHING METHODS

In the process of teaching an educational discipline, in order to acquire certain learning outcomes, to activate the educational process, it is envisaged to use such learning methods as:

Verbal (lectures 1-10), problematic lecture (Topic 11).

Visual (demonstration (Topic 1-11)).

Practical (laboratory work (Topics 1-11)).

FORMS AND METHODS OF ASSESSMENT

The University uses a 100-point accumulative system for evaluating the learning outcomes of students of higher education.

Current control is carried out during lecture, laboratory and has the purpose of checking the level of preparedness of the student of higher education for the performance of specific work and is evaluated by the sum of points scored: for courses with a form of semester control as grading: maximum amount is 100 points; minimum amount required is 60 points.

The final control includes current control and assessment of the student.

Semester control is carried out in the form of agrading.

The final grade in the course is determined:

– for disciplines with a form of grading, the final grade is the amount of all points received during the current control.

During the teaching of the course, the following control measures are used:

Current control: individual educational tasks during laboratory work protection(60 points), two written control papers (40 points).

Semester control: Grading.

More detailed information on the assessment system is provided in technological card of the course.

RECOMMENDED LITERATURE

Main

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсеєв С.П., Король О.Г. – Львів:

«Новий світ-2000», 2019. – 678 с.

2. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с.

3. Інформаційна безпека держави: навчальний посібник / В. М. Рудницький, С. О. Гнатюк, Н. В. Лада, Р. В. Бреус. - Харків : ТОВ «ДІСА ПЛЮС», 2018. – 359 с.

4. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-комунікаційних системах https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

5. Молчанов В. П. Технології розробки WEB-ресурсів [Електронний ресурс] : навч. посіб. / В. П. Молчанов, О. К. Пандорін ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (7,94 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2019. - 129 http://www.repository.hneu.edu.ua/handle/123456789/22466

6. Інформатика в сфері комунікацій [Електронний ресурс] : навч.-практ. посіб : у 3-х ч. Ч. 2 : Обробка та аналіз даних / С. Г. Удовенко, О. В. Тесленко, Н. О. Бринза [та ін.] ; за заг. ред. С. Г. Удовенка; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (14,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2019. - 249 с http://repository.hneu.edu.ua/handle/123456789/23347

Additional

7. Shmatko O. New method for assessing the risk of automated information systems information security based on fuzzy-multiple approach / O. Shmatko, N. Romaschenko. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020. – P. 93–104. http://repository.hneu.edu.ua/handle/123456789/24819

8. Milov O. Creation of a methodology for building security systems for multimedia information resources in social networks / O. Milov, S. Milevskyi, V. Aleksiyev. // Przetwarzanie, transmisja i bezpieczenstwo informacji. – Bielsko-Biala : Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsko-Bialej, 2020. - Vol. 12. - S. 185-192. http://repository.hneu.edu.ua/handle/123456789/24817

9. Synergy of building cybersecurity systems: monograph / Edited by S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. http://repository.hneu.edu.ua/handle/123456789/25623

10. Shmatko O. Information support for distributed teamwork knowledge management / O. Shmatko, M. Bilova. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– P. 169–192. http://repository.hneu.edu.ua/handle/123456789/24818

11. CNA 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

12. EVE - virtual environment in the field of networks, security and DevOps https://www.eve-ng.net/

13. Site of personal educational systems of S. Kuznets Kh NEU in the discipline "Security engineering of information and communication systems" https://pns.hneu.edu.ua/enrol/index.php?id=10074