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

ЗАТВЕРДЖЕНО
на засіданні кафедри
інформаційних систем.
Протокол № 1 від 27.08.2024 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи

_____ Каріна НЕМАШКАЛО

БЕЗПЕКА ІС

робоча програма навчальної дисципліни (РПНД)

Галузь знань	12 "Інформаційні технології"
Спеціальність	126 «Інформаційні системи та технології»
Освітній рівень	другий (магістерський)
Освітня програма	"Інформаційні системи та технології"

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

Розробник:
к.т.н., доцент підписано КЕП Андрій ПОЛЯКОВ

Завідувач кафедри
інформаційних систем _____ Дмитро БОНДАРЕНКО

Гарант програми підписано КЕП Олександр КОЛГАТІН

Харків
2024

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

APPROVED
at the meeting of the Information Systems Department
Protocol № 1 of 27.08.2024

AGREED
Vice-rector for educational and methodical work

_____ Karina NEMASHKALO

SECURITY OF INFORMATION SYSTEMS

Program of the course

Field of knowledge	**12 "Information Technologies"**
Specialty	**126 "Information systems and technologies"**
Study cycle	**second (master's)**
Study programme	**"Information Systems and Technologies"**
Course status	**mandatory**
Language	**English**

Developers:
Cand. Sc. (Technical), Associate Professor, Lecturer — digital signature — Andrii POLIAKOV

Head of Information System Department _____ Dmytro BONDARENKO

Head of Study Programme — digital signature — Oleksandr KOLHATIN

Kharkiv
2024

INTRODUCTION

The course “Security IS” is a key course in the formation of competencies in the field of information systems and technologies protection. In today's information society, where data volumes are growing exponentially and information technologies are penetrating all areas of human activity, the importance of reliable information security cannot be overestimated. The growing number of cyberattacks, their complexity and potential damage require specialists to have in-depth knowledge and skills in protecting information assets. The course is aimed at developing, analyzing and applying comprehensive protection measures that ensure the integrity, confidentiality and availability of information. Particular attention is paid to modern standards and methodologies, cryptographic data protection, methods of mitigating security threats, building a secure software development and deployment process, as well as risk management and access control strategies that are an integral part of modern information systems.

Studying the course “Security IS” involves mastering knowledge of the basic principles of cybersecurity; security standards for processing and storing personal data; application of cryptographic security methods; security as a business problem; mastering the skills of using tools to research modern threats to Web and mobile applications and APIs, as well as creating a secure software development cycle. In addition, it is important to acquire the ability to design and develop IS applications, considering security requirements and protection against modern threats.

The purpose of teaching the course “Security IS” is to provide students with in-depth theoretical knowledge and practical skills in the field of information systems security, including threat identification and analysis, development and implementation of comprehensive security measures, as well as risk management and access control. The course is also aimed at mastering modern technologies and methodologies for data protection, cryptographic information security, network infrastructure security, and software development security.

The objectives of the course are:

provide students with the necessary theoretical knowledge about methods and means of ensuring security in information systems;

development of practical skills in the use of cryptographic security tools;

training students in the skills of protecting Web applications and researching request forgery attacks;

formation of a knowledge system on the current state of threats, attacks and security services;

forming a system of knowledge about international standards and frameworks for data security and security mechanisms;

mastering the principles of construction, purpose, structure of the process of secure software development;

mastering the basic practices of designing and developing multi-level Web-oriented software components with security requirements;

understanding of the basic cryptographic methods and protocols of symmetric / asymmetric encryption, digital signature, data integrity, key management, blockchain;

mastering the skills of modeling threats to an information system.

The subject of the course "Security of Information Systems" is the study of methods, technologies, standards and procedures that ensure the protection of information resources from unauthorized access, modification, disclosure and other threats. The focus is on risk analysis and assessment, access management, cryptographic data protection, as well as network security and software development.

The subject of the course is information systems and networks, their infrastructure, data, software, and operating procedures that need to be protected from 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
LO03	SC06
LO10	GC05, SC03, SC06
LO12	SC06

Note:

LO03. Making effective decisions on the problems of information infrastructure development, creation and application of IT.

LO10. Providing high-quality cyber protection of ICT, to plan, organize, implement and monitor the functioning of information protection systems.

LO12. Improving the information system on the base of business processes analysis.

GC05. Ability to evaluate and provide the quality of the work performed.

SC03. Ability to design information systems taking into account the specifics of their purpose, incomplete/insufficient information and conflicting requirements.

SC06. Ability to manage information risks based on the concept of information security.

COURSE CONTENT

Content module 1: Data and system security methods and standards

Topic 1: Identification and access control

1.1. Security principles.

Identification, authentication, authorization: identifiers, weak / strong authentication, biometric authentication: static / dynamic, authentication token, smart card, certificate, security identifier (SID). Authentication protocols.

1.2. Access control models.

Selective access control, mandate access control, role-based access control, attribute-based access control.

1.3. Methods and technologies of access control,

Separation rules, password, token (authorization), two-factor authentication, multifactor authentication.

1.4. Threats to access control.

Password strength, threats to overcome password protection, privilege acquisition, hidden channels.

1.5. Access control monitoring.

Logging, logged file system, auditing, logging. The concept of entrepreneurship.

Topic 2. Security standards

2.1. Policies, standards, guidelines and procedures. International standards:

ISO/IEC 27001:2013/27002:2013/27005:2015/27006:2015/27005.

2.2. NIST Cybersecurity Framework

2.3. Risk management.

Basic criteria, risk assessment criteria, impact criteria, risk recognition criteria, application and boundary of the risk management organizational structure, risk analysis, risk identification risk measurement.

2.4. Threat modelling.

Risk analysis, threat identification, vulnerability identification asset identification.

2.5. Risk management frameworks.

Topic 3. Definitions and concepts of cryptography

3.1. Encryption methods.

Modern standards of symmetric encryption, strength of symmetric encryption methods, encryption modes.

3.2. Basic principles of asymmetric cryptography.

RSA/ECES asymmetric encryption schemes, Rabin asymmetric encryption scheme, El Gamal asymmetric encryption scheme, Diffie-Hellman protocol.

3.3. Message integrity.

Key and keyless hash functions, MAC/HMAC, Electronic digital signature ECDSA, Group digital signature. Blind digital signature. One-time digital signature. Digital signature standards on the elliptic curve.

3.4. Public key infrastructure.

Certificate usage policy. X.509 public key certificates. Public key infrastructure components and services. Lists of revoked certificates. PKI policy. Problems and risks of PKI technology.

3.5. Cryptographic attacks.

Model of the offender. Requirements for modern cryptographic algorithms. Factorization. Method of factorization of the general sieve of a number field. Methods for solving a discrete logarithm in a group of points on an elliptic curve.

Content module 2: Security of the enterprise information system

Topic 4. Communication and network security

4.1. OSI network model.

Layers of the OSI model: Application layer, Transport layer, Interconnection layer, Network Access Layer, Interaction of layers.

4.2. TCP/IP model.

Comparison with the OSI model, distribution of protocols by TCP/IP layer.

4.3. Network organizations.

Internet service provider, Root DNS.

4.4. Network devices: bridge, switch, router, proxy, VLAN.

4.5. Wireless networks:

IEEE 802.11, organization of Wi-Fi networks, Direct and indirect threats, authentication, encryption in Wi-Fi networks.

4.6. Network encryption.

Building VPN networks. Traffic encryption in the IPSec protocol. Encrypting traffic and ensuring data integrity in the SSL protocol. Encrypting traffic and ensuring data integrity in the TLS protocol. Key management in the IPSec protocol. Validation of TLS/SSL certificates. Integrity and authenticity in the application layer protocols of the OSI model. SSH protocol.

4.7. Network attacks:

DoS attack, DNS attack schemes. DNS flood attacks, DNS server cache attack.

Topic 5. Security of Web and mobile application development

5.1. Threats and methods of attack in Web and mobile applications. OWASP

5.2. Cross-Site Scripting Attack (XSS).

5.3. Cross-Site Request Forgery Attack (CSRF).

5.4. XML External Entity (XXE) attack.

5.5. Injection attacks.

SQL injection, code injection, command injection

5.6. Using third-party dependencies.

Integration methods, package managers, vulnerability and risk database.

Topic 6. Software development security.

6.1. Models of software development.

cascade model, spiral model, non-functional requirements for the system.

6.2. Software development life cycle SDLC.

6.3. Integrating security into SDLC.

Static code analysis, dynamic code analysis, software composition analysis, interactive application security testing.

6.4. Mobile code: security requirements for mobile software applications.

6.5. Database management: security requirements for databases,

6.6. Malware: different types of malwares, attacks and ways to protect the IT system from malware.

The list of practical (seminar) / laboratory studies in the course is given in table 2.

Table 2

The list of practical (seminar)) / laboratory studies

Name of the topic and/or task	Content
Topic 1. Task 1	Investigation of access control methods in the Linux system.
Topic 2-3. Task 2	Investigation of modern cryptographic standards of symmetric cryptography.
Topic 2-3. Task 3	Investigation of modern cryptographic standards of asymmetric cryptography.
Topic 4. Task 4	Investigation of FireWall operation and methods of bypassing it
Topic 5. Task 5	Research of modern attacks on Web applications: CSRF and SQL injection attacks.
Topic 6. Task 6	Research of methods of dynamic and static analysis of software code.

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

Table 3

List of self-studies

Name of the topic and/or task	Content
Topic 1-6	Search, selection and review of literature on a given topic
Topic 1-6	Preparation for laboratory classes
Topic 1-6	Performing an individual task (presentation)
Topic 1-6	Preparing for the current control work

The number of hours of lectures, practical (seminar) studies and hours of self-study is given in the technological card of the course.

TEACHING METHODS

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

Verbal (lecture-discussion (Topic 1 – 4), problem lecture (Topics 4 – 6), lecture-visualization (Topics 1 – 6)).

Visual (demonstration (Topic 5 – 6)).

Laboratory work (Topics 1 – 6), case studies (Topics 4 – 6).

FORMS AND METHODS OF ASSESSMENT

The University uses a 100-point cumulative system for assessing the learning outcomes of students.

Current control is carried out during lectures, practical, laboratory and seminar classes and is aimed at checking the level of readiness of the student to perform a specific job and is evaluated by the amount 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 a semester exam or grading.

The final grade in the course is determined:

– for courses 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: pass of laboratory works (60 points), current control works (20 points), presentations (20 points).

Semester control: Grading.

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

RECOMMENDED LITERATURE

Main

1. В.І. Гур'єв Інформаційна безпека держави: навч. посіб. для студ. спец. «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. — Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2018.

2. Довгань О. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / О. Довгань, Л. Литвинова, С. Дорогих. — К. : Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського, 2023. — 300 р.

3. Ю.Г. Даник ОСНОВИ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. — Одеса : ОНАЗ ім. О.С. Попова, 2019. — 320 р.

Additional

4. Ю. І. Горбенко Прикладна криптологія. Теорія. Практика. Застосування / Ю. І. Горбенко, І. Д. Горбенко. — Харків : Видавництво «Форт», 2012. — 870 р.

5. Домарев, В. В. Безпека інформаційних технологій. Системний підхід / В. В. Домарев. - К .: ДиаСофт, 2004.

6. R. Ross, M. McEvilley and J. C. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, 2016.

7. Ross R. Developing Cyber-Resilient Systems:: A Systems Security Engineering Approach / R. Ross, V. Pillitteri, R. Graubart, [та ін.]. — Gaithersburg, MD : National Institute of Standards and Technology, 2021. — NIST SP 800-160v2r1 p.

8. ДСТУ ISO/IEC 15946-3:2006 Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина

3. Встановлення ключів (ISO/IEC 15946-3:2002, IDT).

9. В. Ю. Зубок, Кібербезпека топології INTERNET : монографія / В. Ю. Зубок,, В. В. Мохор. — К. : ІПМЕ ім. Г.Є.Пухова, 2022. — 191 р.

Information resources

10. Cybersecurity Framework / NIST. — 2024. Available at: https://www.nist.gov/cyberframewor.

11. TechRepublic: News, Tips & Advice for Technology Professionals [Електроний ресурс] // TechRepublic. — Електрон. дані. — Режим доступу: https://www.techrepublic.com/.

12. Основні ресурси | Ваша повна бібліотека з кібербезпеки [Електронний ресурс] // KnowledgeFLOW. — Електрон. дані. — Режим доступу: https://knowledgeflow.org/uk/resources/.

13. Index Top 10 - OWASP Top Ten 2021 : Related Cheat Sheets [Електроний ресурс] // OWASP Cheat Sheet Series. — Електрон. дані. — Режим доступу: https://cheatsheetseries.owasp.org/IndexTopTen.html.

14. OWASP WSTG - Web Security Testing Guide [Електронний ресурс] // Latest | OWASP Foundation. — Електрон. дані. — Режим доступу: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/.

15. Server Side Request Forgery [Електронний ресурс] // OWASP Foundation. — Електрон. дані. — Режим доступу: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery.

16. Server Side Request Forgery Prevention [Електронний ресурс] // OWASP Cheat Sheet Series. — Електрон. дані. — Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html.