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

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**12 Інформаційні технології**
Спеціальність	**121 Інженерія програмного забезпечення**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**Інженерія програмного забезпечення**

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

Розробник(и):
д.т.н., проф. підписано КЕП Сергій СЕМЕНОВ

д.т.н., проф. Ольга СТАРКОВА

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

Гарант програми
к.т.н., доц. Олег ФРОЛОВ

Харків
2024

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

PROGRAM AND DATA SECURITY

Program of the course

Field of knowledge	**12 Information technologies**
Specialty	**121 Software engineering**
Study cycle	**first (bachelor)**
Study programme	**Software Engineering**

Course status	**mandatory**
Language	**English**

Developer: Dr. Sc. (Engineering), prof.	digital signature	Serhiy SEMENOV
Dr. Sc. (Engineering), prof.		Olha STARKOVA
Head of Cybersecurity and Information Technologies Department		Olha STARKOVA
Head of Study Programme		Oleg FROLOV

Kharkiv
2024

INTRODUCTION

Today, information protection is turning into one of the most urgent tasks due to the extremely wide spread of various information processing systems, as well as the expansion of local and global computer networks, which transmit huge volumes of information of a state, military, commercial, and private nature, the owners of which often would be categorically against introducing it to outsiders. The problem becomes particularly acute after the government of Ukraine adopted the law on personal data protection, which obliges to store and transfer personal data of employees only in a protected form in information systems (IS).

An equally important task is the wide implementation of information technologies in various spheres of human activity in Ukraine: the rapid growth of the circulation of plastic cards, the future introduction of electronic passports and medical cards, student tickets and score books; eventually, more and more government institutions and private enterprises switch to electronic document management, which, moreover, requires the legal validity of the signature of an individual or legal entity. The proliferation of such technologies also, of course, requires well-designed information protection.

The purpose of teaching the course is to teach students the principles of building complex information protection systems, research and use of modern procedures for providing basic information security services in banking systems, which are based on the use of symmetric and asymmetric cryptography algorithms in communication systems, public key infrastructure (PCI) protocols.

The objectives of the course are to acquire skills: analysis of potential threats to basic information security services, assessment and management of effective protection of information and information systems in the modern digital environment.

The subject of the course is the security of programs and data.

The object of the course is technical means, software products, processes and methods used to ensure information security in systems.

The results of the study of this course are the acquisition of skills in the use of methods of encryption of information for its further transmission through telecommunication communication channels.

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

Table 1

Learning outcomes and competences formed by the course

Learning outcomes	**Competencies**
LO13	SC06
LO21	GK02, SK06, SK07, SK10

where, GK02.Ability to apply knowledge in practical situations;

SK06. Ability to analyze, select and apply methods and tools to ensure information security (including cyber security);

SK07. Knowledge of data information models, ability to create software for data storage, extraction and processing;

SK10. The ability to accumulate, process, and systematize professional knowledge about creating and maintaining software and recognize the importance of life long learning;

LO13. Know and apply methods of developing algorithms, designing software and data and knowledge structures;

LO21. To know, analyze, select, and competently apply information security (including cyber security) and data integrity tools in accordance with the applied tasks and software systems being developed.

COURSE CONTENT

Topic 1. Basic concepts and definitions of cyber security

1.1. The role of information in the world, the importance of protection.

1.2. Information protection services and mechanisms.

Topic 2. Fundamentals of cryptography. Simple encryption algorithms

2.1. Terminology.

2.2. History of cryptography.

2.3. Modern cryptography.

2.4. Encryption and decryption.

Topic 3. Authentication protocols. Digital signature.

3.1. A classic problem of cryptography.

3.2. Cryptoanalysis.

Topic 4. PGP system.

4.1. A brief description of the functions of the PGP system

4.2. The principle of the system.

4.3. Sending and receiving PGP messages.

4.4. Generic PGP message format.

Topic 5. Algorithms for ensuring data integrity

5.1. Private-public key relationships.

5.2. Degrees of trust in the PGP system

5.3. Sending and receiving PGP messages

Topic 6. Ensuring data security at the network level

6.1. Redundancy of code.

6.2. Code with parity check.

6.3. Hamming code.

Topic 7. Ensuring data security at the network level

7.1. Technologies and standards of the physical layer 802.11
7.2. Security of wireless networks
7.3. Vulnerability of the WEP algorithm
7.4. Basic authentication

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

Table 2

The list of laboratory studies

Name of the topic and task	Content
Topic 1. Laboratory work 1. The simplest ciphers.	Basic principles of operation of the simplest ciphers; elements of cryptanalysis, in particular frequency analysis of cryptograms.
Topic 2. Laboratory work 2. Block symmetric ciphers.	Ensuring confidentiality and integrity of information using block symmetric ciphers;
Topic 3. Laboratory work 3. Asymmetric cryptosystems.	Use of asymmetric encryption mechanisms to ensure confidentiality of messages.
Topic 4. Laboratory work 4. Digital signature algorithm	Application and research of a digital signature system using asymmetric crypto transformations.
Topic 5. Laboratory work 5. Steganographic methods of information protection	The main methods of steganography information protection, use of appropriate software.
Topic 6. Laboratory work 6. Using PGP to encrypt email messages	Email security software with encryption and digital signature.
Topic 7. Laboratory work 7. "Statistical studies of generators of random and pseudo-random sequences according to the NIST STS method"	Methods of researching statistical properties of generators of random and pseudo-random sequences.

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	Basic concepts and definitions of cyber security
Topic 2. Task 2.	Fundamentals of cryptography. Simple encryption algorithms
Topic 3. Task 3.	Authentication protocols. Digital signature
Topic 4. Task 4.	The PGP system
Topic 5. Task 5.	A study of the PGP system
Topic 6. Task 6.	Algorithms for ensuring data integrity
Topic 7. Task 7.	Ensuring data security at the network level of the 802.11 network.

The number of hours of lectures, laboratory studies and hours of self-study is given in the technological card of the course.

TEACHING METHODS

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

Verbal (lectures 1-7), problematic lecture (Topic 1).

In person (demonstration (Topic 1-7)).

Practical (laboratory work (Topics 1-7)).

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, laboratory 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 grading.

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: performance and defense of laboratory works (7 works with 10 points each), written tests (3 works with 10 points each).

Semester control: Grading.

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

RECOMMENDED LITERATURE

Main

1. Лісовська, Ю. П. Інформаційна безпека України : навчальний посібник для студентів вищих навчальних закладів / Ю. П. Лісовська. - Київ : Кондор, 2020. - 170 с.

2. Michael E. Whitman Principles of Information Security 6th Edition / Michael E. Whitman, Herbert J. Mattord - Cengage Learning; 6th edition (March 13, 2017) 656 p.

3. Richard E. Smith Elementary Information Security 3rd Edition / Jones & Bartlett Learning; 3rd edition (October 28, 2019) – 708 p.

4. Євсеєв, С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. Електрон. текстові дан. (12,3 МБ). Харків : ХНЕУ ім. С. Кузнеця, 2020. 221 с.:

іл. Загол. з титул. екрану. Бібліогр.: с. 211-213. http://repository.hneu.edu.ua/handle/123456789/24508

5. Milov O. Self-organizing organizational structures of cybersecurity systems / O. Milov, V Aleksiyev. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko]. Vienna: Premier Publishing s.r.o., 2020. P. 65-78. http://repository.hneu.edu.ua/handle/123456789/24816

Additional

6. Jason Andress Foundations of Information Security: A Straightforward Introduction / No Starch Press (October 7, 2019) – 248 p.

7. Якименко І.З. // Опорний конспект лекцій з дисципліни “Безпека програм та даних” для студентів спеціальності “Кібербезпека”. – Тернопіль, 2019. – 50 с.

8. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

9. Martovytskyi V. Technology for monitoring the functioning state of distributed computer systems / V. Martovytskyi, Y. Koltun, D. Holubnychyi et al. // Системи управління, навігації та зв’язку : зб. наук. пр. – 2022. – Вип. 1 (67). – С. 75-80. http://www.repository.hneu.edu.ua/handle/123456789/27369.

Information resources

10. EVE - віртуальне середовище в області мереж, безпеки та DevOps https://www.eve-ng.net/

11. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Безпека програм та даних" https://pns.hneu.edu.ua/course/view.php?id=10208