Національний технічний університ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ І
імені ІГОРЯ СІКОРСЬКОГО»

"Національний технічний університет України "Київський політехнічний інститут"

Department of Computer Engineering

PROTECTION OF INFORMATION IN COMPUTER SYSTEMS AND NETWORKS

(Syllabus)

Details of the academic discipline

Level of higher education	*First (undergraduate)*
Branch of knowledge	*12 Information technologies*
Specialty	*123 Computer engineering*
Educational program	*Computer systems and network*
Discipline status	*Mandatory (normative) component of OP, professional training cycle*
Form of education	*full-time / part-time*
Year of training, semester	*4th year, autumn*
Scope of the discipline	*4.5 credits / 135 hours*
Semester control/ control measures	*Examination*
Timetable	*http://rozklad.kpi.ua/*
Language of teaching	*Ukrainian*
Information about head of the course / teachers	*Lecturer: Doctor of Technical Sciences, Professor Oleksii Oleksandrovich Pisarchuk, kga46826@gmail.com.*
Placement	*https://drive.google.com/drive/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d?usp=sharing* *https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg*

• Program

1. Description of the educational discipline, its purpose, subject of study and learning outcomes

The discipline "Information protection in computer systems and networks" is intended for students to acquire the ability to ensure the protection of information processed in computer and cyber-physical systems and networks in order to implement the established information security policy. This is achieved by studying the theoretical foundations of the construction and practice of applying methods and means of information protection in computer systems in order to prevent unauthorized access, leakage, destruction, destruction and modification of information of various categories through the implementation of policies and the creation of complex corporate information protection systems.

The purpose of studying the course "Information Protection in Computer Systems and Networks" is: acquisition by students of the ability to ensure the protection of information processed in computer and cyber-physical systems and networks in order to implement the established information security policy.

The discipline provides the following learning outcomes of the educational and professional program Computer systems and networks: ZK2, ZK8,, FC1, FC4, FC6, FC7, FC8, FC9, FC13, FC16, FC17, FC19, PRN3, PRN6, PRN9, PRN10, PRN20.

2. The goal of the course is achieved by the implementation of partial tasks:

1. Study of the main provisions of the legal framework in the field of information protection in computer systems: national legislative acts and standards in the field of information protection: categories, main provisions, procedure and scope of application; legislative acts and standards of other states in the field of information protection - 1 lecture;

2. Determination of the composition, organizational, technical and software and hardware means of the complex system of protection of corporate information: information as an object of protection; categories of information as an object of protection; corporate information leakage channels; information threats in computer systems; model of the offender; methods, methodologies, means, measures and technologies of complex protection of corporate information (organizational measures, technical protection of information, countering technical means of monitoring) - 2 lectures, 1 laboratory work (2 hours);

3. Computer viruses and virology: classification of viruses; algorithms of functioning of viruses; technologies and means of creating and spreading computer viruses; virus constructors; antivirus software and the essence of its construction and application; methods and technologies for protecting computer systems from viruses - 2 lectures, 1 laboratory work;

4. Cyber threats to computer systems and their countermeasures: cyber and (and) computer attack, concepts, classification, model, content of stages; methods and technologies of organizing and implementing cyber attacks; methodologies, methods and technologies for countering cybernetic attacks; and, software method and the essence of its construction and application; methods and technologies for protecting computer systems from viruses - 2 lectures, 1 laboratory work;

5. Cryptographic protection of information in computer systems: general information about classical cryptology, cryptography and cryptographic analysis; traditional historical ciphers; block encryption algorithms; principles of construction of modern symmetric cryptographic ciphers and systems; asymmetric cryptographic encryption systems (essence and mathematical foundations; algorithms and cryptographic systems; implementation technologies and vulnerability) – 9 lectures, 4 laboratory work;

6. Methods, methodologies, technologies and means of authentication and identification as an element of information protection in computer systems: methods and technologies of user identification; electronic digital signature, electronic key certification centers - 2 lectures, 1 laboratory work.

3. According to the results of studying the course, the student should know:

The main provisions of the legal framework in the field of information protection in computer systems: national legislative acts and standards in the field of information protection: categories, main provisions, procedure and scope of application; legislative acts and standards of other states in the field of information protection.

Composition of organizational, technical and software and hardware means of a comprehensive system of corporate information protection: information as an object of protection; categories of information as an object of protection; corporate information leakage channels; information threats in computer systems; model of the offender; methods, methodologies, means, measures and technologies of comprehensive protection of corporate information (organizational measures, technical protection of information, countering technical means of monitoring;

Principles of construction, action and protection against computer viruses and the basics of virology: classification of viruses; algorithms of functioning of viruses; technologies and means of creating and spreading computer viruses; virus constructors; antivirus software and the essence of its construction and application; methods and technologies for protecting computer systems from viruses;

Methods, stages, methods and means of carrying out cybernetic attacks on computer systems, methods, means and technologies of countering them: cybernetic and (and) computer attack, concepts, classification, model, content of stages; methods and technologies of organizations

5. Educational materials and resources

Base:

1._Daemen J. AES Proposal: Rijndael, AES Algorithm Submission [Electronic resource] / J. Daemen, V. Rijmen. – Access mode : http://www.docstoc.com/docs/14641406/AES-Implementation-and-Performance-Evaluationon-8-bit-Microcontrollers._

2.Department of Defense Trusted Computer System Evaluation Criteria [Electronic resource]. – Access mode : http://www.dynamoo.com /orange/fulltext.htm.

3.D.VAM.1 Performance Benchmarks. Revision 1.1 / R. Avanzi, B. Chevallier-Mames etc. // In: ECRYPT Research report IST-2002-507932. European Network of Excellence in Cryptology / M. Joye ed. – August, 3, 2015. – 87 p.

4.ISO/IEC 7498-2:1989 – Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture [Electronic resource]. – Access mode : http://www.iso.org/iso /catalogue_detail.htm?csnumber=14256.

5.NESSIE consortium "NESSIE Security report." Deliverable report D20 – NESSIE, 2002. – NES/DOC/ENS/WP5/D20 [Electronic resource]. – Access mode : http://www.cryptonessie.org/

Information resources:

- [https://drive.google.com/drive/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d?usp=sharing].
- https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg
- [http://195.78.68.84/dsszzi/control/uk/doccatalog/list?currDir=41640].

● Education content

6. Methods of mastering the academic discipline

Chapter 1. Basic information about information protection in computer systems.

Topic 1. Basic provisions of the legislative framework in the field of information protection in computer systems:

content and tasks of the discipline;

national legislative acts and standards in the field of information protection: categories, main provisions, procedure and scope of application;

legislative acts and standards of other states in the field of information protection.

Chapter 2. Organizational, technical, and software and hardware means of a comprehensive system of corporate information protection.

Topic 2. Comprehensive system of protection of corporate information. Object of protection and threats:

information as an object of protection;
categories of information as an object of protection;
corporate information leakage channels;
information threats in computer systems;
Topic 3 Comprehensive system of protection of corporate information. Composition and structure:
model of the offender;
methods, methodologies, means, measures and technologies of comprehensive protection of corporate information (organizational measures, technical protection of information, countering technical means of monitoring).
Chapter 3. Computer viruses and virology.
Topic 4. General information about computer viruses:
classification of viruses;
algorithms of functioning of viruses;
technologies and means of creating and spreading computer viruses.
Topic 5. Technologies for protecting computer systems against computer viruses:
virus constructors;
antivirus software and the essence of its construction and application;
methods and technologies for protecting computer systems from viruses.
Chapter 4. Cyber threats to computer systems and their countermeasures.
Topic 6. Methods and means of implementing cyber attacks:
cybernetic and (i) computer attack, concepts, classification, model, content of stages;
methods and technologies of organizing and implementing cyber attacks.
Topic 7. Methods and means of combating cybernetic attacks:
methodologies, methods and technologies for combating cybernetic attacks (methods, software and the essence of its construction and application);
methods and technologies for protecting computer systems from viruses.
Chapter 5. Cryptographic protection of information in computer systems.
Section 5.1. General information about cryptography and cryptology.
Topic 8. General information about classical cryptology, cryptography and cryptographic analysis:
General information about encryption, coding, cryptography and cryptology;
Deciphering problems;
Technologies and systems of cryptographic protection of information.
Topic 9. Traditional historical ciphers. Mathematical and algorithmic foundations:
General information and fields of application.
Encryption based on one and many alphabetic substitutions: Caesar and "wanderer" ciphers;
Viginer cipher and Wheatstone squares.
Bigram ciphers.
Stream ciphers with unlimited key length.
Encryption by "braking".
Topic 10. Traditional historical ciphers. Implementation technologies and vulnerability:
Implementation of traditional historical ciphers using Python tools;
Examples of implementation of traditional ciphers in Python;
Vulnerability of traditional historical ciphers.
Section 5.2. Methods, models, algorithms and systems of block encryption.
Topic 11. Algorithms of block encryption. Mathematical and algorithmic foundations:
The essence and mathematical foundations of block encryption methods.;
Topic 12. Algorithms of block encryption. Implementation technologies and vulnerability:
Block encryption technologies in Python, vulnerability.
Section 5.3. Methods, models, algorithms and systems of symmetric encryption.
Topic 13. Symmetric ciphers and systems. Mathematical and algorithmic foundations:
Encryption based on alternating permutations and substitutions;
Data Encryption Standard. (DES).

Topic 14. Symmetric ciphers and systems. Implementation technologies and vulnerability:

Key control unit in DES. 3-DES algorithm and four modes of implementation of DES-based cryptographic protection.

Asymmetric encryption technologies in Python, vulnerability.

Section 5.5. Methods, models, algorithms and systems of asymmetric encryption.

Topic 15. Asymmetric ciphers and systems. Mathematical and algorithmic foundations:

Cryptography according to Diffie and Hellman. Irreversible functions in encryption. Three schemes and problems of cryptoprotection.

RSA system. Modular arithmetic. Algorithm of fast discrete potentiation. Processor – RSA accelerator;

Asymmetric encryption technologies in Python, vulnerability.

Topic 16. Asymmetric ciphers and systems. Implementation technologies and vulnerability:

The problem of generating large prime numbers (LPG). Rabin's test and Fermat's little theorem. Simplicity checks.

Key calculation schemes and algorithms for the RSA system. Classical and advanced algorithms of Euclid.

Asymmetric encryption technologies in Python, vulnerability.

Chapter 6. Methods, methodologies, technologies and means of authentication and identification.

Topic 17. Methods and technologies of user identification in distributed computer systems:

methods of authentication and identification of subjects based on symmetric encryption systems. Concept of master key and variable key;authentication and identification technologies in PythonТема 18.Electronic digital signature, methods and means:

establishing message integrity based on symmetric and asymmetric encryption systems. Concept of message signature and digital signature;

authentication and identification of subjects in protocols of open orders. The concept of electronic checks and receipts;

multi-level organization of formation and use of encryption keys. Functions of the master key, system, client, trade-cash and session keys.

The cycle of laboratory work in the discipline "Information protection in computer systems" is aimed at acquiring practical skills in the implementation and research of the features and effectiveness of the components of a complex system of corporate information protection, both in the form of individual elements and in a synergistic combination into a single system.

The cycle of laboratory works is built on the principles of increasing the functionality of the complex system of corporate information protection. This is implemented in several aspects:

heuristic synthesis of a complex corporate information protection system;

researching the features of computer viruses and creating a countermeasure system;

study of the peculiarities of cybernetic influence on computer systems and the creation of a countermeasure system;

development of cryptographic information protection systems and research of their vulnerability.

Issues of virology and cyber security are practiced on real malware using virtual computing technologies.

The issue of developing cryptographic information protection systems and researching their vulnerability is implemented using the capabilities of the high-level programming language - Python.

Topics of laboratory work:

Laboratory work #1. (2 hours) Study of the processes of creating a comprehensive system of corporate information protection:

Development of a project of CSPI for a specific object of information activity - a computer system (establishment of the category of information to be protected; study of leakage channels, threat model; model of the violator; a set of organizational and technical measures and means of information protection; structure of CSPI; study of effectiveness of CSPI) .

Laboratory work #2. (2 hours) Study of information protection processes against computer viruses:

Creating an isolated virtual research environment; generation of viruses and research of their signatures; research on the effectiveness of detecting virus signatures with various software tools; creating a system for protecting information from computer viruses and researching its effectiveness.

Laboratory work #3. (2 h.) Study of information protection processes against cybernetic attacks:

Creating an isolated virtual research environment; study of the vulnerability of the environment to cybernetic influences; creating a system for protecting information from cybernetic influences and researching its effectiveness.

Laboratory work #4. (2 hours) Study of traditional encryption technologies and their vulnerabilities:

Development of a script in Python that implements traditional encryption technologies according to a given algorithm and studies their vulnerability.

Laboratory work #5. (2 hours) Study of block encryption technologies and their vulnerabilities:

Development of a script in Python that implements block encryption technologies according to a given algorithm and studies their vulnerability.

Laboratory work #6. (2 hours) Study of symmetric encryption technologies and their vulnerabilities:

Development of a script in Python that implements symmetric encryption technologies according to a given algorithm and studies their vulnerability.

Laboratory work #7. (2 hours) Study of asymmetric encryption technologies and their vulnerability:

Development of a script in Python that implements asymmetric encryption technologies according to a given algorithm and studies their vulnerability.

Laboratory work #8. (2 hours) Research of authentication and identification technologies in distributed computer systems:

Development of a Python script that implements electronic digital signature technologies and research into the effectiveness of authentication and identification processes in distributed computer systems.

7. **Individual work**

The student's independent work includes preparation for classroom classes, calculations based on primary data obtained in laboratory classes, solving problems, and performing modular control work. The total amount of time allocated to independent work is 66 hours.

Politic and control

8. Politic

In the process of studying the academic discipline, the following is welcomed and encouraged:

- *collegiality of mutual relations in the process of implementing the educational process;*
- *timeliness of reporting on all forms of control;*
- *compliance with norms of academic integrity.*

The procedure for filing and providing reports on all forms and the procedure for evaluating results is regulated by the procedure specified in the tasks: for laboratory work; modular control work; methodical materials for the calculation.

9.Types of control and rating system for evaluating learning outcomes (RSE)

RSE in the discipline, the semester control of which is provided in the form of an exam, is developed according to the RSO-2 type and consists of two components:

- *initial – intended for evaluation of current control measures during the semester (Rc*
- *examination - intended for evaluating individual questions (tasks) on the exam. (Re)*

The recommended size of the starting component of RSO is equal to 60 points, the examination component - 40 points.

Starting points are formed as a sum of rating points received by the applicant based on the results of current control measures, incentive and penalty points.

After evaluating the applicant's answers on the exam (or completing the exam control work), the teacher summarizes the starting points and the points for the exam, reduces them to a rating grade and transfers them to grades on the university scale.

$$R = Rc + Re$$

Types of control in the academic discipline:

1. *Execution and defense of 8 laboratory works.*
2. *Performance of test work*
3. *Examination.*

Table 1

Assessment of individual types of student academic work (in points)

Mode		Total
Performance and protection of laboratory work № 1		6
Performance and protection of laboratory work № 2		6
Performance and protection of laboratory work № 3		6
Performance and protection of laboratory work № 4		6
…		
Performance and protection of laboratory work № 8		8
Performing laboratory work	**R1**	50
Test	**Rk**	10
Total in semester	**Rc= R1 + Rк**	**60**
Examination	**Re**	**40**
Total in semester	: (**R = Rc + Re**)	**100**

1. Execution and defense of 8 laboratory works

*Maximum score for one work is 6-8. The maximum number of points for all laboratory works is equal to 6 * 7 + 8 = 50 points.*

1.1. Neat design of the protocol of laboratory work - 2 points.

1.2. Timely protection of work - 1 point.

1.3. Complete work (theoretical justification, practical result, analysis and conclusions) – 6-8 points.

2. Test

The maximum number of points for the test is 10 points.

3. Examination

The maximum number is 40 points.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Points	*Raiting*
100-95	*Perfectly*
94-85	*Very well*
84-75	*Okay*
74-65	*Satisfactorily*
64-60	*Enough*
<60	*Unsatisfactorily*
Admission conditions not met	*Not allowed*

10. Additional information on the discipline (educational component)10

The list of questions submitted for semester control

List of theoretical questions.

1. Reveal the essence of the concepts: information protection; comprehensive information protection system; information threats.

2. What is information security, what does it include?

3. Reveal the essence and components of technical information protection.

4. Describe the national legislation in the field of information protection.

5. Describe the standards of other countries in the field of information protection.

6. Properties of information.

7. Categories of information.

8. Threats of information.

9. Model of the violator.

10. Threat model.

11. Security policy.

12. Comprehensive information protection system.

13. Classification of viruses.

14. Algorithm of work of file viruses.

15. Reveal the essence of the work of macroviruses.

16. Virus detection methods.

17. Types of antivirus programs.

18. Criteria for the effectiveness of antivirus programs.

19. Composition of the computer virus protection system.

20. Classification and characteristics of remote control software.

21. What is a computer attack and its stages.

22. Types and scenarios of computer attacks.

23. Reveal the content of the preparatory stage of a computer attack.

24. To reveal the content of the preparatory stage of the implementation of a computer attack.
25. Reveal the content of the preparatory final stage of a computer attack.
26. Classification of software protection against computer attacks.
27. Protection against computer attacks using firewalls.
28. Security scanner. Essence, purpose, functioning.
29. Comprehensive information protection system against computer attacks.
30. Technology of virtual private networks as a means of protection against computer attacks.
31. Criteria for the effectiveness of antivirus programs.
32. Information protection technologies using crypto-algorithms.
33. Conveyor of cryptographic protection tasks and their essence.
34. Classification of cipher algorithms.
35. Explain the essence of the concepts: cryptology, coding, encryption of information
36. Essence, purpose, types of classical ciphers.
37. Performance indicators of crypto-algorithms.
38. The essence, algorithm, advantages and disadvantages of the Caesar cipher.
39. The essence, algorithm, advantages and disadvantages of the wandering cipher.
40. The essence, algorithm, advantages and disadvantages of the Wigener cipher.
41. The essence, algorithm, advantages and disadvantages of the Wheatstone cipher.
42. The essence, algorithm, advantages and disadvantages of stream ciphers
43 The essence, algorithm, advantages and disadvantages of encryption by the gamming method.
44. Cryptographic analysis. The main implementation methods and their essence.
45. Block encryption algorithms - essence, properties, implementation.
46. Characteristics of stability of block encryption algorithms.
47. Stream encryption algorithms: essence, examples, implementation.
48. Modern crypto-algorithms of symmetric encryption.
49. Symmetric cryptographic systems and their standards.
50. Asymmetric cryptographic systems and their standards.
51. Technologies of authentication and identification in computer systems.
52. Implementation of authentication and identification technologies using an electronic digital signature.
53. Vernam Cipher;
54. Encryption by the method of inhibition.
55. Permutation ciphers:
56. Permutation ciphers without using keys;
57. Permutation ciphers using keys.
58. Generators of random sequences for cryptographic systems.
59. Data Encryption Standard (DES) symmetric block encryption standard.
60. Multi-cascade DES algorithm.
61. IDEA's symmetric block data encryption algorithm
62. Cryptographic system RSA.

List of practical questions.
1. To develop a comprehensive information protection system for the object of information activity - the local computer network of the laboratory for the development of applied software in the banking sector, which includes 5 officials.

2. Develop a model of the violator and a model of threats to the object of information activity - the local computer network of the laboratory for the development of applied software in the field of national security and defense, which includes 8 officials.
3. To develop a technical task for the creation of KSZI at the object of information activity - a local computer network of the laboratory for the development of applied software in the field of automation of production process management, which includes 12 officials.
4. Develop a system of information protection against its leakage through technical channels at the object of information activity - the local computer network of the laboratory for the development of cryptographic information protection systems, which includes 22 officials.
5. To develop a system for combating cyber threats at the object of information activity - a local computer network with access to global networks, used in a software development laboratory based on distributed high-speed computing technologies. The laboratory includes 15 officials.
6. Develop a system for combating cyber threats at the object of information activity - a local computer network for access to global networks, used in a software development laboratory using distributed technologies
7. To develop a complex information protection system at the object of information activity - a local computer network for access to global networks, used in a software development laboratory based on distributed high-speed computing technologies. The laboratory includes 12 officials.
8. Develop a cryptographic system and its software component using the Caesar cipher. English text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
9. To develop a cryptographic system and its software component using a wandering cipher. English text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
10. Develop a cryptographic system and its software component using the Wigener cipher. English text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
11. Develop a cryptographic system and its software component using the Wheatstone cipher. English text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
12. Develop a cryptographic system and its software component using a double Caesar cipher. Ukrainian text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
13. To develop a cryptographic system and its software component using a double wandering cipher. Ukrainian text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
14. Develop a cryptographic system and its software component using a double Wigener cipher. Ukrainian text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
15. Develop a cryptographic system and its software component using a double Wheatstone cipher. Ukrainian text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
16. Develop a cryptographic system and its software component using an affine cipher. Ukrainian text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
17. Develop a cryptographic system and its software component using an affine cipher. English text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.

18. Develop a cryptographic system and its software component using a double affine cipher. Ukrainian text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
19. Develop a cryptographic system and its software component and its software component using a double affine cipher. English text files are subject to encryption. Carry out a cryptographic analysis of the developed cryptographic system.
20. Develop a cryptographic system and its software component using the stream RC4 cipher. Ukrainian text files are subject to encryption.
21. Develop a cryptographic system and its software component using the stream RC4 cipher. English text files are subject to encryption.

Working program of the academic discipline (syllabus):

Compiled by Oleksiy Oleksandrovich Pisarchuk, professor of the Department of Computer Science, Doctor of Technical Sciences.

Approved by the Department of Computing (Protocol No. 10 dated 05/25/2022).

Agreed by the Methodical Commission of the Faculty of Informatics and Computer Engineering (protocol No. 10 dated 06/09/2022).

…