Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Department Computer Engineering

SECURITY SYSTEM OF PROGRAMS AND DATA

(Syllabus)

Реквізити навчальної дисципліни

Level of higher education	First (undergraduate)
Branch of knowledge	12 Information technologies
Specialty	123 Computer engineering
Educational program	Computer systems and networks
Discipline status	Selective (professional training cycle)
Form of education	full-time (full-time), part-time
Year of training, semester	3rd year, spring semester
Scope of the discipline	4 credits/120 hours
Semester control/ control measures	Test , MKR
Timetable	http://rozklad.kpi.ua/Schedules/ScheduleGroupSelection.aspx
Language of teaching	English
Information about head of the course / teachers	associate professor OT, Ph.D., Volokita Artem Mykolayovych,
Placement	comsys.kpi.ua bbb.comsys.kpi.ua

Program

1. Description of the educational discipline, its purpose, subject of study and learning outcomes навчальної дисципліни, її мета, предмет вивчення та результати навчання

The credit module "Security system of program and data" is designed to study methods and means of managing access to information carriers and databases, modern standards and encryption tools for building complex systems for protecting computer systems and networks from intrusions. The credit module is designed to study design methods and techniques for configuring software and technical means of protection of operating systems, which ensure the creation of highly protected distributed computer systems.

The credit module is related to the materials studied in the following credit modules:

- discrete mathematics (NF-05)
- software engineering (ZP-02)
- system programming (ZP-04)
- computer architecture (NP-03)
- parallel and distributed computing (ZP-07).
- operating systems (NP-04)
- computer networks (NP-05)
- computer systems (NP-06)

The material of this credit module will be used when studying the following credit modules:

- automated design of computer systems (ZP-09)
- pre-diploma practice (NP-10),
- diploma design (NP-11).

II. DISTRIBUTION OF EDUCATIONAL TIME

The distribution of study hours by semesters and types of study sessions is carried out in accordance with the working study plans in the following form:

SEMESTER COD	Total	*Hours*							MCW	Individual work	Final test
		Lecture	*Practic*	*Seminars*	*Labs*	*Комп'ютерний практикум*	*ISW*				
							Total	*Individual work student*			
7/3П-9	120	36	-	–	18	-			1	66	Test

III. M PURPOSE AND OBJECTIVES OF THE CREDIT MODULE

The purpose of studying the credit module "Information protection in computer systems" is for the student to acquire practical design and programming skills when creating complex systems or special hardware and software subsystems to protect information from unauthorized access based on:

- the ability to formalize and use the legal framework for information protection in automated systems, methods and means of access management to distinguish the rights of users to information with limited access,
- assimilation of standard means and encryption algorithms for the construction of software and technical support for cryptographic protection of particularly important information and the formation of the necessary key encryption base.
- the ability to solve analytical tasks of generating large prime numbers, calculating keys and cryptographic resistance of modern symmetric and asymmetric encryption systems and determining their basic characteristics.
- acquisition of techniques for creating and insisting on appropriate software and technical support for the protection of information resources of automated systems;.

The student should know:

the main concepts of creating demonstrably sufficient information protection systems, Adept-50, Bella-Lapadula and other models, existing mechanisms for implementing protection models that are implemented in various operating systems based on "mandate lists" and "access lists", ways of implementing the principles of "extension of rights access" and "minimum privileges", standards, algorithms and modes of implementation of cryptographic protection of information, methods and means of generating encryption keys, protocols and stages of authentication of subjects and messages in open communication channels, protocols of conferences and open orders, structure and characteristics of electronic payment systems and plastic payment cards, requirements of well-known standards regarding classification and criteria for the protection of computer systems against unauthorized access to information in terms of confidentiality, integrity, availability, controllability.

The student should be able to:
perform the final stages of design when creating or modifying information protection subsystems against unauthorized access and preventing intrusions into computer systems, take into account the requirements for passwords and evaluate the basic characteristics of password protection systems, write a set of programs for discrete management of access to information on media or the site, determine evaluations complexities of software or hardware implementation of symmetric and asymmetric algorithms of cryptographic protection, DES, 3-DES, SHA, SSL, RSA, El-Gamale and others algorithms, evaluate the cryptoresistance of algorithms, apply methods and algorithms for forming digital signatures and key certificates, develop a graphical administrator interface security, configure information protection programs, organize their placement and execution on workstations and in the computer network.

IV. PLAN

IV.I. DISTRIBUTION OF EDUCATIONAL TIME BY TOPICS

	Mode of work						
Name	*Всього*	*Lecture*	*Practice*	*Seminars*	*Labs*	*Computer practice*	*ISW*
Chapter 1. Introduce	**4**	**2**					**2**
Topic 1.1 Problems of information protection in computer systems and networks (CSM).		1					1
Topic 1.2 Main directions of threats to the NSD and channels of information leakage from the KSM. Targets, subjects and schemes of active and passive intrusions		1					1
Chapter 2. A comprehensive approach to the creation of information protection systems in computer systems.	**8**	**4**					**4**
Topic 2.1 Regulatory framework of information protection. The main directions and means of information protection in KSM.		1					1
Topic 2.2 Models of provably sufficient information protection systems. Adept-50 concept models,. Denning, Landwehr.		1					1
Topic 2.3 The matrix		1					1

model of the Bell and La Padula protection system. Concept of subject, rights vector and access manager. Extension of access rights.							
Topic 2.4. Model of the KSM safety monitoring system. Concept of threat factor and statistical anomaly.		1					1
Chapter 3. Identification of subjects and access control based on a password system.	**16**	**4**			**8**		**4**
Topic 3.1 User identification based on the password system. Password requirements. Password storage scheme in Unix OS.		1			2		1
Topic 3.2 Analysis of the characteristics of the system of simple passwords. Anderson's formula. Examples.		1			2		1
Topic 3.3 Modifications of the password system. Confirmation of access rights based on the unilateral and bilateral "handshake" procedure.		1			2		1
Topic 3.4 Logs: registration and operational. Logging-based security monitoring on Unix and Windows		1			2		1
Chapter 4. Discrete delimitation of subjects' access to information in the limited matrix model of the protection system.	**4**	**2**					**2**

Topic 4.1 Access lists and formation of user categories. Inheritance of rights. Locks, keys and access conditions in the VAX/VMS OS.		1					1
Topic 4.2 Mandate lists and implementation of the "minimum privileges" principle. Mandatory access in Unix OS.		1					1
Chapter 5. Computer approaches to cryptographic protection of information with limited access.	**6**	**4**					**2**
Topic 5.1 Encryption based on one and many alphabetic substitutions. Concept of cipher and secret key. Caesar's Cipher		1					
Topic 5.2 Encryption based on permutations. Problems of decryption and cryptanalysis		1					1
Topic 5.3 Bigram ciphers. Viginer cipher and Wheatstone squares. Encryption machines		1					
Topic 5.4 Stream Ciphers with Unlimited Key Length. Encryption by "throwing".		1					1
Chapter 6. Symmetric encryption in communication systems with open communications.	**12**	**4**			**4**		**4**
Topic 6.1 Organization of data transfers in secret systems according to Shannon. Means of entropy		1					1

maximization.							
Topic 6.2 Encryption based on alternating permutations and substitutions. The Lucifer System.		1					1
Topic 6.3 Federal encryption standard Data Encryption Standard. (DES). General scheme and masking function with keywords.		1			2		1
Topic 6.4 Key management unit in DES. 3-DES algorithm and four modes of implementation of DES-based cryptographic protection.		1			2		1
Chapter 7. Asymmetric encryption systems based on public and secret keys.	**20**	**6**			**8**		**6**
Topic 7.1 A new direction in cryptography according to Diffie and Hellman. Irreversible functions in encryption. Three schemes and problems of cryptoprotection.		1			2		2
Topic 7.2 The RSA system. Modular arithmetic. Algorithm of fast discrete potentiation. The processor is an RSA accelerator.		1			2		2
Topic 7.3. The problem of generating large prime numbers (LPG). Rabin's test and Fermat's little theorem. Simplicity checks.		2			2		1
Topic 7.4. Key calculation schemes and algorithms for the RSA system. Classical		2			2		1

and advanced algorithms of Euclid. Examples							
MCW	**2**	**1**					**1**
Chapter 8. Increasing cryptoresistance in asymmetric encryption systems.	**6**	**3**					**3**
Topic 8.1 Estimates of cryptoresistance of the RSA algorithm. Comparison with DES and 3-DES schemes. Examples		1					2
Topic 8.2 El-Gamal encryption system. Key calculation schemes and algorithms for the El-Gamal system. Examples of encryption and decryption		2					1
Chapter 9. Authentication of subjects and establishment of "trust" relationship in distributed systems and networks.	**16**	**4**			**6**		**6**
Topic 9.1 Establishing "trust" of subjects based on symmetric encryption systems. Communication establishment protocols.		1			2		1
Topic 9.2. Establishing "trust" of subjects based on asymmetric encryption systems. The concept of a public key certificate.		1			2		2
Topic 9.3 Establishing message integrity based on symmetric and asymmetric encryption systems. Concept of digital signature.		1			2		1
Topic 9.4 Organization of		1					2

"trust" communication in protocols of "open orders". The concept of electronic checks and receipts.							
Chapter 10. Electronic payment systems. Means of increasing the "trust" of virtual relations.	**8**	**2**					**6**
Topic 10.1 Plastic cards as a basis for the organization of electronic payments. Issuing banks and acquiring banks.		1					1
Topic 10.2 Structure of the electronic payments system. POS terminals. Functions and organization of the processing center.		1					1
Topic 10.3 Multi-level organization of formation and use of encryption keys.							2
Topic 10.4 Electronic trade based on E-business technology. SSL and SET protocols. Hierarchy of signatures in trust relations.							2
Preparation for the test	12						12
Test	4						4
Total:	**120**	**36**	**-**	**-**	**18**		**66**

IV.2 LECTURES

Chapter 1. Introduction

Lecture 1. Problems of information protection in computer systems and networks (CSM). The concept of unauthorized access (USA), KSM vulnerability, intrusion threat, information leakage channel. The main directions of threats to the NSD and the channels of information leakage from the KSM. Targets, subjects and schemes of active and passive intrusions.
[1, c.56-57; 2, p. 63-68].

Chapter 2. A comprehensive approach to the creation of information protection systems in computer systems.

Lecture 2. Regulatory and legal basis of information protection. The concept of information with limited access and protection systems. The main directions and means of information protection in

KSM. Models of provably sufficient information protection systems. Adept-50 concept model. Concept of object and category. Denning's model. Concept of security domain. Landwehr model. The concept of the perimeter of responsibility. [3, c. 31-33; 2, p. 53-54, 74-77, 121-122].

Lecture 3. The matrix model of the Bell and La Padula protection system. Concept of subject, rights vector and access manager. Extension of access rights. Model of the KSM safety monitoring system. Concept of threat factor and statistical anomaly. Anomaly indication vector. [1, c.78-84, 58-62; 2, p. 69-73, 90-92, 117-120].

Chapter 3. Identification of subjects and access control based on a password system.

Lecture 4. User identification based on the password system. Password requirements. Password storage scheme in Unix OS. Analysis of the characteristics of the system of simple passwords. Anderson's formula. Examples.. [1, c 65-70. ; 2, p. 104-107].

Lecture 5. Modifications of the password system. Confirmation of access rights based on the unilateral and bilateral "handshake" procedure. Logs: registration and operational. Logging-based security monitoring on Unix and Windows.
[1, c. 71-72; 2, p. 108-112].

Chapter 4. Discrete delimitation of subjects' access to information in the limited matrix model of the protection system.

Lecture 6. Access lists and formation of user categories. Inheritance of rights. Locks, keys and access conditions in the VAX/VMS OS. Mandate lists and implementation of the "minimum privileges" principle. Mandatory access in Unix OS. [1, c117-123. ; 2, p. 134-138].

Chapter 5. Computer approaches to cryptographic protection of information with limited access.

Lecture 7. Encryption based on one and many alphabetic substitutions. Concept of cipher and secret key. Caesar's Cipher. Permutation-based encryption. The code "wandered". Problems of decryption and cryptanalysis. [1, c.78-84, 58-62; 2, p. 69-73, 90-92, 117-120].

Lecture 8. Bigram ciphers. Viginer cipher and Wheatstone squares. Encryption machines. Stream ciphers with unlimited key length. Encryption by "throwing". [3, c. 31-33; 2, p. 53-54, 74-77, 121-122].

Chapter 6. Symmetric encryption in communication systems with open communications.

Lecture 9. Organization of data transfers in secret systems according to Shannon. Means of entropy maximization. Encryption based on alternating permutations and substitutions. The Lucifer System. [1, c 65-70. ; 2, p. 104-107].

Lecture 10. Data Encryption Standard. (DES). General scheme and masking function with keywords. Key control unit in DES. 3-DES algorithm and four modes of implementation of DES-based cryptographic protection. [1, c. 71-72; 2, p. 108-112].

Chapter 7. Asymmetric encryption systems based on public and secret keys.

Lecture 11. A new direction in 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. The processor is an RSA accelerator. [1, c117-123. ; 2, p. 134-138].

Lecture 12. The problem of generating large prime numbers. Rabin's test and Fermat's little theorem. Simplicity checks. Examples. [1, c. 71-72; 2, p. 108-112].

Lecture 13. Key calculation schemes and algorithms for the RSA system. Classical and advanced algorithms of Euclid. Examples. [1, 134-136c.].

Chapter 8. Markov models of mass service systems.

Lecture 14. Estimates of the cryptoresistance of the RSA algorithm. Comparison with DES and 3-DES schemes. Examples. [1, c.78-84, 58-62; 2, p. 69-73, 90-92, 117-120].

Control work from chapters 2 - 7.

Lecture 15. El-Gamal encryption system. Key calculation schemes and algorithms for the El-Gamal system. Examples of encryption and decryption.. [3, c. 31-33; 2, p. 53-54, 74-77, 121-122].

Chapter 9. Authentication of subjects and establishment of "trust" relationship in distributed systems and networks.

Lecture 16. Establishing "trust" of subjects based on symmetric encryption systems. The concepts of master key and variable key. Communication establishment protocols. Establishing "trust" of subjects based on asymmetric encryption systems. The concept of a public key certificate. Communication establishment protocols. [1, c 65-70. ; 2, p. 104-107].

Lecture 17. Establishing message integrity based on symmetric and asymmetric encryption systems. Concept of message signature and digital signature. Organization of "trust" communication in the protocols of "open orders". The concept of electronic checks and receipts. [1, c. 71-72; 2, p. 108-112].

Chapter 10. Electronic payment systems. Means of increasing the "trust" of virtual relations.

Lecture 18. Estimates of the cryptoresistance of the RSA algorithm. Comparison with DES and 3-DES schemes. Examples. The structure of the electronic payments system. POS terminals. Functions and organization of the processing center. [1, c.78-84, 58-62; 2, p. 69-73, 90-92, 117-120].

IV.5 LABS

The purpose of conducting a cycle of laboratory work is for students to acquire the necessary practical skills for developing and researching mock-up samples of information protection subsystems, which are the embodiment of effective approaches and algorithms for creating a comprehensive system of information protection against unauthorized access, researching the characteristics of the necessary data structures, developing and debugging individual components of the console interface security administrator under Linux, WindowsXP, FreeBSD using Delphi, Java, C++, Assembler languages for researching protection mechanisms in automated systems of various purposes.

Laboratory work includes:

- formulation of the input problem,

- theoretical information on methods and means of problem solving,
- analysis of mathematical and algorithmic support,
- justification of the choice of research software,
- development of a structural diagram of interaction of protection subsystems,
- results of step-by-step algorithm verification,
- interpretation of results and conclusions,
- program listing.
- results of model experiments
- interpretation of modeling results and conclusions,
- program listing.

Laboratory work 1. Development and research of a software subsystem for discrete control of access to a separate information carrier with a complex directory structure.
Laboratory work 2. Programming and research of user identification subsystem based on simple passwords with requirements control and log support.
Laboratory work 3. Programming and research of the user authentication subsystem during operation using "questions-answers" and secret functions.
Laboratory work 4. Programming and research of the monitoring subsystem to detect anomalies and dangerous events related to protected information.
Laboratory work 5. Development of a software layout for research and step-by-step verification of the algorithm of fast discrete potentiation and other operations with arbitrary length of operands.
Laboratory work 6. Development of a software layout for the study and step-by-step verification of algorithms for generating large prime numbers with the formation of an HPV database.
Laboratory work 7. Development of a software layout for research and step-by-step verification of RSA - key management subsystem, encryption and decryption of messages.
Laboratory work 8 Development of a software layout for research and step-by-step verification of DES - subsystems of signature formation, encryption and decryption of messages.

IV.7 CONTROL WORK

Control work 1. Topics: 3.2, 4.2., 7.2, 7.3, 7.4, 8.1..

The purpose of the work: to check the results of studying techniques for analyzing the characteristics of password and cryptographic protection subsystems, calculating large prime numbers, and determining secret and public encryption keys.

V. METHODICS

The educational work program of the discipline for the correspondence form of education should include cool works that compensate for the limited time of laboratory work.

VI. EDUCATIONAL AND METHODOLOGICAL MATERIALS

LIST OF BASIC LITERATURE

1. Weissman C. Security Controls in the ADEPT-50 Time Sharing System. // Proceedings AFIPS, FJCC. – 2010. – v. 35. – pp. 119-133.
2. Hartson R., Hsiao D. Full protection specification in the semantic model for database protection languages. // Proceedings Annual Conference ACM. – Houston, New York. – 2014. – pp. 90-95.

LIST OF ADDITIONAL LITERATURE

4 Harrison M. A.. Russo W. L. Protection in Operating Systems. // Communications of the ACM. – 2014. – v. 19, № 8. – pp. 461-471.

5 Spier M. J. A Model Implementation for protective domains. // International Journal on Computer Information Science. – 2021. – v. 2, № 3. – pp. 201-229.

6 Bell D. E., LaPadula L. J. Secure computer systems: mathematical foundations and model. // M74-244, The MITRE Corp., Bedford, Mass.- May 1999.

7 Bell D. E. Secure computer systems: a refinement of the mathematical model. // Springfield, The MITRE Corp. – 2018. – Report № 2574, pp. 75

8 Graham R. M., Denning P. J. Protection – Principles and Practice. // Proceedings AFIPS. – 2018. – v.40, pp. 417-429.

10 Denning D. E. A Lattice Model of Secure Information Flow. // Communications of the ACM. – 2011. – v. 19, № 5. – pp. 236-243

11 Landwehr C., Heitmeyer C., McLean J. A security model for military message systems. // ACM Trans. on Computer Systems. – 2017. – V. 2, № 3. – pp. 198-222.

Table of correspondence of rating points to grades on the university scale:

Rating **R**	***Traditional credit assessment***
100-95	perfectly
94-85	very well
84-75	good
74-65	satisfactorily
64-60	enough
< 60	unsatisfactorily
Admission conditions not met	not allowed

Working program of the academic discipline (syllabus):

Compiled by Artem Mykolayovych Volokita, Ph.D., associate professor.

Approved by the Department of Computing (protocol No_10_from 05/25/2022).

Agreed by the Methodical Commission of the faculty (protocol No. 10 dated 06.9.2022).