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

ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека та захист інформації***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

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

Розробник:
к.т.н., доцент _____ Олена ШАПОВАЛОВА

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ Ольга СТАРКОВА

Гарант програми _____ Вячеслав ЛИМАРЕНКО

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

FUNDAMENTALS OF CRYPTOGRAPHIC PROTECTION

Program of the course

Field of knowledge	***12 Informational technologies***
Specialty	***125 Cyber security and information protection***
Study cycle	***first (bachelor)***
Study programme	***Cyber security***
Course disciplines	**mandatory**
Language	**English**

Developer:
PhD (Engineering),
Associate Professor _____ Olena SHAPOVALOVA

Head of Cybersecurity and
Information Technology
Department _____ Olga STARKOVA

Head of Study Programme _____ Viacheslav LYMARENKO

Kharkiv
2023

INTRODUCTION

It should be noted that today security issues, in particular in cyberspace, are extremely important. In terms of doing business, learning, communicating online, this applies to absolutely everyone: objects of strategic importance, commercial enterprises, average citizens, and one of the key points of organizing secure communication and data transmission is the use of an arsenal of cryptographic methods and tools.

This CAD contains a detailed plan of lectures of the course "Fundamentals of cryptographic protection" by modules and topics, a list of laboratory classes. Revolutionary changes of the last decade that took place in Internet resources, led to the unification of information and computer networks into a single informational and cybernetic space, which prompted the creation of an information- corporate networks on basis internet technologies, which significantly expanded spectrum of electronic services in society both for everyone in general and for private use separately. As consequence, significant threats to such an information resource as an Internet resource (IR) have also transformed. IR security threats have acquired signs of hybridity. Manifestations of signs of hybridity as a result of simultaneous exposure threats of informative security, cybernetic safety (CS) and safety information (SI) on IR brought to occurrence phenomena synergy, negative manifestations which in need cardinal viewing concepts constructions of the current ones systems security.

Dissemination Internet technologies also requires well placed protection of information, which circulates in cyberspace. So study basic mechanisms of software safety, software protection on each cycles its existence is allocated many attention.

The purpose of the course is to give students the knowledge and skills for studying and mastering in the future disciplines related to information security and its processing, to a large extent determines the level of general scientific training of specialists and forms the basic basis for studying the principles, methods, algorithms and computing technologies for processing information with limited access.

Tasks course is:

- receiving practical skills in using cryptography to protect and save information;
- obtaining knowledge about the application of the latest methods of information protection at deployment and functioning applications;
- familiarization with the possibilities of providing reliable protection in the conditions of the post-quantum period.

The object of the course are cryptographic methods of information protection and tools for its organization.

The subject of the course is hardware and software tools and mathematical apparatus for the implementation of cryptographic methods for information protection.

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**
LO 2	GC 1, GC2, GC 4, GC 5
LO 3	GC 1, GC2, GC 4, GC 5
LO 4	GC 1, GC2, GC 4, GC 5
LO 10	GC 1, PC 2, PC 11
LO 14	PC 2, PC 3, PC 5, PC 8, PC 10, PC 11
LO 15	PC 2, PC 3, PC 11
LO 18	GC 1, PC2, PC 3, PC5, PC11
LO 19	GC 1, PC 2, PC 5, PC 8, PC 11
LO 23	PC 5 , PC 6, PC 8, PC 11
LO 24	GC 1, PC 4 , PC 5, PC 9, PC 11
LO 31	PC 2, PC 6, PC 10
LO 32	GC 1, PC 4 , PC 5, PC 8, PC 11
LO 40	PC 10
LO 47	PC 2, PC 3, PC 5, PC 10
LO 48	PC 5, PC 6 , PC 8, PC 10, PC 11

where GC 1 is an ability to apply knowledge in practical situations;

GC 2 is the knowledge and understanding of the subject area and understanding of the profession;

GC 4 is an ability to identify, pose and solve problems in a professional sphere;

GC 5 is an ability to search, process and analyze of information;

PC 2 is an ability to use information and communication technologies, modern methods and models of information security and/or cyber security;

PC 3 is an ability to use software and software-hardware complexes of information protection means in the information and telecommunication (automated) systems;

PC 5 is an the ability to ensure the protection of information processed in the information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy;

PC 6 is an the ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks and failures of various classes and origins;

PC 8 is an ability to carry out incident management procedures, conduct investigations, provide them with an assessment;

PC 9 is an ability to carry out professional activities based on the implemented information and/or cyber security management system;

PC 10 is an ability to apply methods and means of cryptographic and technical protection of information at objects of information activity;

PC 11 is an ability to monitor the functioning of information, information and telecommunication (automated) systems according to the established policy of information and/or cyber security;

LO 2 is to organize one's own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;

LO 3 is to use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity;

LO 4 is to analyze, argue, make decisions in the process of solving complex specialized tasks and practical problems in professional activities, which are characterized by complexity and incomplete determination of conditions, to be responsible for the decisions made;

LO 10 is to perform analysis and decomposition of information and telecommunication systems;

LO 14 is to solve the task of protecting programs and information processed in information and telecommunication systems by means of hardware and software and to evaluate the effectiveness of the quality of the decisions made;

LO 15 use modern software and hardware of information and communication technologies;

LO 18 is to use software and software-hardware complexes for the protection of information resources;

LO 19 is to apply theories and methods of protection to ensure information security in information and telecommunication systems;

LO 24 solve the problems of managing access to information resources and processes in information and information-telecommunication (automated) systems based on access control models (mandate, discretionary, role);

LO 23 is to implement measures to counter unauthorized access to information resources and processes in information and information and telecommunication (automated) systems;

LO 31 is to apply theories and methods of protection to ensure the safety of elements of information and telecommunication systems;

LO 32 is to solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the established security policy;

LO 40 is to interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information protection system;

LO 47 is to solve the problems of protecting information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information;

LO 48 is to implement and support intrusion detection systems and use

cryptographic protection components to ensure the required level of information security in information and telecommunication systems.

COURSE CONTENT

CONTENT MODULE 1. PROTECTION MECHANISMS BASED ON SYMMETRIC AND ASYMMETRIC ALGORITHMS

Topic 1. Theoretical foundations of information protection.

Basic definitions. A set of data protection tools. Security policies. Approaches to ensuring the protection of information of ASIO

Cryptographic transformation of information and cryptographic protection. Cryptographic analysis.

Source authentication. The main tasks of the security system.

Symmetric cryptosystems. Nonlinear replacement nodes of symmetric crypto-algorithms . Block and current algorithms. Performance indicators of cryptographic Boolean functions (non-linear replacement nodes).

Double and triple DES algorithms . Advanced Encryption Standard (AES). RIJNDAEL algorithm. Algorithm of symmetric block transformation "Kalyna-256".

Operating modes of block encryption algorithms ISO/IEC 10116:1997. Electronic code book mode (electronic code book mode).

ciphertext feedback modes (ciphertext feed back mode). Output feedback mode (output feed back mode).

Asymmetric encryption schemes. NP - complete tasks. Factorization of a number, discrete logarithm in a group of points of an elliptic curve, decoding of a random code.

Asymmetric RSA system. Diffie-Hellman key exchange system . Authentication and confidentiality protocol.

Topic 2. Protocols of authenticity. Digital signature.

Mechanisms for ensuring authenticity . Classification and methods of organization of digital signatures.

RSA digital signature. Digital signature: STANDARD DSA, DSS, DSTU R-3410.

Hashing methods. Keyless and keyed hash functions. Unilateral (one - way hash function (OWHF)) and collision-resistant hash functions (SCHF). Hash function DSTU 7564 (" Kupina - n").

Schemes on modular transformations. Scheme of MASH-1 hashing algorithm . CBC - MAC ISO / IEC 6796 hash function.

Specialized hash functions. Secure Hash Algorithm . Hash functions from the RIPEMD family.

Authentication mechanisms: based on the use of software and hardware; in the TSR/IP stack. KERBEROS server authentication system.

Authentication using certificates. Passage of IP data packet (transport and tunnel modes).

Topic 3. Strict authentication protocols

Algorithms and protocols of two-factor authentication (2 FA).

PASSWINDOWS strict authentication method: limitations of the software implementation of the algorithm. 2FA PASSWINDOWS monitoring algorithm.

Authentication Trust Levels: Requirements and Limitations. Threats in case of two-factor authentication

Multi-factor authentication. RSA SecurID technology .

Two-factor authentication in LINUX. Google settings authenticator for each user.

SSH settings. Ensuring SSH security.

Topic 4. SSL/TLS integrity protocols.

Integrity protocols SSL, TLS. A synergistic model of fusion threats on CCISI on PCS.

Structure, functions and versions of the SSL protocol. Using the SSL protocol. Structure, functions and versions of the TLS protocol. Using the TLS protocol.

Attacks on SSL/TLS: "CHOSEN PLAINTEXT" (WEI DAI). "PADDING ORACLE" (SERGE VAUDENAY), POODLE. Attacks on the HANDSHAKE protocol.

Record Layer in TLS 1.3: AEAD encryption. Encryption with CHACHA20. Authenticated encryption. Encryption method using the Galois field : AES-GSM. Principle and algorithm of work.

A combination of CHACHA20 and POLY1305 stream cipher capabilities. The I2P project (Invisible Internet Project). I2P networks. Tunneling .

New transport protocol NTCP2. Changes in ROUTERINFO. Generation of data transmission keys during connection establishment.

Galois fields . The structure of finite fields and their properties. Galois fields on rings of polynomials. Basic properties of Galois fields .

Topic 5. PGP system.

The concept of the PGP system and its functions. PGP services: authentication, confidentiality, digital signature, interoperability.

Requirements for keys in the PGP system. Key identifiers. Creating messages in PGP.

Ensuring trust in PGP. PGP certificates. Operations for determining the degree of trust.

Topic 6. Basics of PKI technology.

Key distribution algorithms. Open Key Infrastructure Components and Services. Certified centers and their functions. Register and archive of certificates. Services. PKI architecture and topology. Interaction of PKI components. PKI standards and specifications.

Software and technical complex "Key Certification Center" and its components.

Classification of keys. Key hierarchy and crypto period.

Life cycle of key management. Key management models. Options for using the key transfer center.

Certification process model.

Diffie-Hellman key matching . Key management mechanisms based on the use of asymmetric methods.

CONTENT MODULE 2. PROTECTION MECHANISMS IN THE

CONDITIONS OF THE POST-QUANTUM PERIOD

Topic 7. Basics of post-quantum cryptography.

Combined cryptosystems.. Specificity of SSL\TLS protocols in the post-quantum period.

SET and HTTPS protocols in the post-quantum period.

Moore's law. Shor's algorithm . Quantum bits.

Quantum objects and entangled states. Quantum acceleration of calculations.

Quantum computer D-WAVE. Quantum Fourier transform. Grover's algorithm .

Quantum key distribution. Polarization of photons. Other key distribution protocols. Attacks on quantum protocols.

Wisner's quantum money .

Subhash protocol Kaka _ Means of mitigating the consequences of the post-quantum breakthrough.

Topic 8. Post-quantum algorithms based on McAlis and Niederreiter crypto - code constructions . Hybrid protection systems based on lossy codes.

Requirements for crypto algorithms of the post-quantum period. Cryptographic types (as ranked by the NIST competition). Quality assessment indicators.

Candidates for the new post quantum standard of asymmetric cryptography. Classification of crypto-code structures

Sydelnikov's attack on crypto-code structures. Niederreiter's crypto-code construction on ES.

Algorithm of balanced coding. Methods of modification of interference-resistant codes

Modified crypto-code structures on MES. The results of the study of the properties of crypto-code structures.

Inferior cryptography, methods of harm. Choosing the best way to inflict damage.

Methods of building hybrid crypto-code structures. An exchange protocol based on McAlice's GCCC .

The results of GKKK research on unprofitable codes.

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

Table 2

The list of laboratory studies

Name topics and / or task	Content
Topic 1. Laboratory work 1	Study of properties and modes work block ciphers
Topic 2. Laboratory work 2	Research protocols authenticity and confidentiality by using RSA
Topic 3. Laboratory work 3	Study of digital protocols signature
Topic 4. Laboratory work 4	Research protocols PGP systems
Topic 5-6. Laboratory work 5	NIST methodology. About prices statistical properties cryptographic algorithms
Topic 7-8. Laboratory work 6	Work with qubits Emulation measurements

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

Table 3

List of self-studies

Name topics and / or task	Content
Topic 1 - 8	Study lecture material and a more in-depth look at the resources referenced in the lecture
Topic 1 - 8	Preparation to laboratory classes
Topic 1 - 8	Preparation to exam

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

TEACHING METHODS

During course teaching process for acquisition defined the application of learning results, activation of the educational process it is provided such methods as

verbal (lecture (Topic 1, 2, 3, 4, 5, 6), problematic lecture (Topic 7, 8));

visual (demonstration (Topic 1–8));

practical (laboratory work (Topic 1–8)).

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 and 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 an exam: maximum amount is 60 points; minimum amount required is 35 points.

The final control includes current control and an exam.

Semester control is carried out in the form of a semester exam.

The final grade in the course is determined: for disciplines with a form of exam, the final grade is the amount of all points received during the current control and the exam grade.

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

Current control: laboratory work (50 points), written control work (10 points).

Semester control: Grading including Exam (40 points).

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

An example of an exam card and assessment criteria.

An example of an examination ticket
Simon Kuznets Kharkiv National University of Economics
First (bachelor) level of higher education
Specialty 125 "Cyber security and information protection"
Educational and professional program "Cyber security"
Semester V
Educational discipline " Fundamentals of cryptographic protection "

EXAMINATION TICKET No. 1

1	Choose the correct continuation of the phrase from the two options Information security is… a. The state of information being stored, processed, or transmitted b. A set of targeted actions and measures.
2	Choose one or more correct answers from the list In which encryption algorithm is the Euler function used? a. RSA b. DES c. GOST 28147-89 d. TripleDES
3	Choose one or more correct answers from the list In which cryptography section are elliptic curves not used? a. Symmetric encryption. b. Asymmetric encryption. c. Electronic digital signatures. d. Symmetric and asymmetric encryption
4	Choose one or more correct answers from the list The requirements for ciphers are: a. Low crypto resistance b. Ease of encryption and decryption procedures c. Sensitivity to the smallest mistakes
5	Choose one answer from the list Is the statement about openness of encryption/decryption algorithms true for asymmetric systems? a. So b. No c. Partly
6	Choose one or more correct continuations of the phrase from the given options The hash function… a. intended to increase the quality of the signed document b. takes an arbitrary-length message as an argument and returns a fixed-length hash value c. The value of the hash function does not depend on the text and allows you to recover the document itself

7	Choose one or more correct answers from the list The key length for the DES symmetric block cipher is ... a. 256 b. 128 c. 56 d. 32
8	Choose one or more correct answers from the list The function of the key system control center does not include... a. Generating keys. b. Creation of certificates. c. Creation of algorithms for electronic digital signatures. d. Key management.
9	Choose one or more correct answers from the list In which of the encryption modes using block algorithms is it possible to parallelize calculations? a. ECB b. CBC c. CFB d. OFB
10	Choose the correct continuation of the phrase Wernham's system proposed in 1917 is: a. Unconditionally stable (theoretically undecipherable) b. Calculated-stable (guaranteed stability) c. Presumably stable (proof-stable) d. Calculated-unstable (time stability)
11	Choose the correct continuation of the phrase Cryptoanalysis by the "birthday" method is a. Probabilistic method b. Analytical method
12	Choose one or more correct answers from the list The number of data conversion cycles for the DES symmetric block cipher is a. 64 b. 16 **c.** 32
13	Choose one or more correct answers from the list A realized security threat is: a. Information security breach b. Attack on information processing facilities c. Finding and exploiting this or that vulnerability
14	Choose the correct continuation of the phrase RSA's cryptographic strength is based on… a. Complexities of factorization of large numbers b. The difficulties of finding a discrete logarithm
15	Choose the correct continuation of the phrase The methodology for building asymmetric cryptosystems is based on the application of: a. Stable modern crypto-algorithms b. Unidirectional functions

16	Choose the correct continuation of the phrase A mechanism for ensuring the integrity and authenticity of the message for symmetric systems a. Digital signature b. The formation of an imitation insert
17	Choose the correct continuation of the phrase The possibility of proving the fact of forgery of a message in case of compromise of the sender on the part of the recipient for asymmetric systems a. Exist b. Does not exist
18	Choose the correct continuation of the phrase Computationally stable cryptosystems are a. Cryptosystems that cannot be revealed by cryptanalysis at all, even with the available unlimited computing and time capabilities of the cryptanalyst b. In order to break such cryptosystems, huge computing and time capabilities are required to carry out a cryptoattack based on a complete enumeration of options
19	Choose the correct continuation of the phrase The bases p and q for the algorithm should be... a. Large prime numbers of the same length b. Mutually prime numbers of different lengths c. Any large numbers
20	Choose the correct option Violation of authority is... a. Penetration threat b. The threat of implementation in. Basic threats

Protocol N dated _____ 20___ was approved at the meeting of the department of CIT.

Examiner PHD, as. prof. Shapovalova Olena

Head of department prof. Starkova Olga

Evaluation criteria

The final marks for the exam consist of the sum of the marks for the completion of all tasks, rounded to a whole number according to the rules of mathematics. The exam contains 20 equivalent questions. For each correct answer - 2 points.

RECOMMENDED LITERATURE

Main

1. Yevseyev S. Research of collision properties of the modified UMAC algorithm he crypto-code constructions / S. Yevseiev , A. Havrylova , O. Korol , O. Dmitriiev , O. Nesmiian , Y. Yufa , A. Hrebennikov // EUREKA: Physics and Engineering . – 2022. – No. 1 (38). - P. 34-43. http://repository.hneu.edu.ua/handle/123456789/26814

2. 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 Bielsku-Bialej, 2020. - Vol. 12. http://repository.hneu.edu.ua/handle/123456789/24817

3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.) http://repository.hneu.edu.ua/handle/123456789/22547

Additional

4. Havrylova A. Development of a pseudo-random substrate for the UMAC algorithm he crypto-code constructions / A. Havrylova , A. Tkachov , A. Shmatko // Information protection and information systems security : proc . of of VIII- th International Scientific and Technical Conference , Lviv , November 11-12, 2021. – Lviv: Polytechnic Publishing House 2021. – P. 49-50 http://repository.hneu.edu.ua/handle/123456789/26840

5. Yevseyev S. Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes / S. Yevseiev , O. Korol , O. Veselska , S. Pohasii , V. Khvostenko // International science and practice conf . "Information security and information technologies", Kharkiv - Odesa, September 13-19 . 2021: Mater. conf . – Kharkiv: KHNEU named after S. Kuznetsa , 2021. - P. 144-157. http://repository.hneu.edu.ua/handle/123456789/26827

6. Encrypt Pad https://evpo.net/encryptpad/#when-encryptpad

7. Tutorial SSH: Understanding Encryption, Ports and Connection https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-workSocial Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples (ISSN: 2523-3246) on 28 April. doi:10.1186/s42400-021-00094-6) https://arxiv.org/ftp/arxiv/papers/2106/2106.01157.pdf

8. What is the difference between SSL vs. TLS? Which Gives Your Website the Best Protection? https://www.websitepulse.com/blog/ssl-vs-tls-difference-and-best-protection

Informational resource

9. Site of personal educational systems of Khnei National University named after S. Kuznets of the academic discipline "Fundamentals of cryptographic protection" https://pns.hneu.edu.ua/course/view.php?id=9688