MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
LUTSK NATIONAL TECHNICAL UNIVERSITY
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

APPROVED
Dean of the Faculty
_____ Inna KONDIUS
29.08.2026

APPROVED
First Vice-Rector
_____ Nadiia KOVALCHUK
29.08.2026

SYLLABUS

of the educational component "Applied Cryptology and Steganography"
higher education degree – Bachelor
field of knowledge – 12 Інформаційні технології
specialty – 125 Кібербезпека та захист інформації
educational programme – Cybersecurity

Кафедра кібербезпеки

Syllabus developed by Associate Professor, PhD Mykola POLISHCHUK

The syllabus was approved at the meeting of the Кафедра кібербезпеки, minutes No. 2 of 28.08.2026

Head of the Department PhD, Associate Professor Serhii KOSTIUCHKO

Reviewed and approved by the support group of the educational programme "Cybersecurity", minutes No. 2 of 28.08.2026

Guarantor of the educational programme "Cybersecurity" PhD, Associate Professor Serhii KOSTIUCHKO

Approved by the Scientific and Methodological Council of the University, minutes No. 1/a of 29.08.2026

Approved syllabus online:
https://e.lntu.edu.ua/syllabus/4143

Lutsk – 2026

SYLLABUS OF THE EDUCATIONAL COMPONENT "Applied Cryptology and Steganography"

Educational programme	Cybersecurity
Field of knowledge / Specialty	12 Інформаційні технології / 125 Кібербезпека та захист інформації
Level of higher education	first (bachelor's)
Course status	compulsory
Language of instruction	English
Workload	5 ECTS credits / 150 hours, semester 7
Form of final assessment	exam
Lecturer(s)	PhD, Associate Professor Mykola POLISHCHUK

1. Course aim and objectives

Aim: Studying this academic discipline contributes to the development of competence among future specialists in the field of modern cryptographic information protection technologies for computer systems; this is achieved through students' practical mastery of skills in working with the latest information technologies in the realms of security and research.

Objectives: The program focuses on training students in the theoretical and practical foundations of modern cryptography and cryptographic information protection within computer systems, fostering practical proficiency in the latest security-related information technologies. It defines the scope of knowledge to be mastered by students at the first (bachelor's) level—in accordance with educational and qualification requirements—as well as the sequence for studying the course material, the necessary methodological resources, and the components and methods for assessing student learning outcomes.

Prerequisites: Information Protection Algorithms and Systems Programming, Information Theory and Coding

2. Competences

GC01 — The ability to apply knowledge in practical situations.

SC05 — The ability to ensure the protection of information processed within information and telecommunication (automated) systems, for the purpose of implementing an established information and/or cybersecurity policy.

SC09 — The ability to carry out professional activities based on an implemented information and/or cybersecurity management system.

SC10 — The ability to apply methods and means of cryptographic and technical information protection at facilities where information-related activities are conducted.

3. Course structure, distribution of hours, links between topics and competences

No.	Topic	Lectures full-time/ part-time	Lab. full-time/ part-time	Self-study full-time/ part-time	Total	Teaching methods	Assessment methods	GC and SC
Content module 1. Fundamentals of Cryptology, Cryptography, and Cryptanalysis								

No.	Topic	Lectures full-time/ part-time	Lab. full-time/ part-time	Self-study full-time/ part-time	Total	Teaching methods	Assessment methods	GC and SC
1	Topic 1. Basic Concepts of Cryptology	2/0.25	2/1	9/14	13/15.25	TM1, TM2, TM5	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05
2	Topic 2. General Information on Information Protection in Information and Telecommunication Systems	4/0	2/1	9/14	15/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05
3	Topic 3. Fundamentals of C. Shannon's Theory of Secret Communication	4/0.25	4/1.75	9/13	17/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC09, SC10
4	Topic 4. Encryption and Public Key Infrastructure	2/0.25	4/0.75	9/14	15/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05, SC10
5	Topic 5. Cryptographic hash functions	2/0.25	2/0.75	9/14	13/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05, SC09, SC10
Content module 2. Data integrity and reliability								
6	Topic 6. Encryption	4/0.25	4/0.75	9/14	17/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05
7	Topic 7. Use of digital signatures	2/0.25	4/1.75	9/13	15/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC10, SC09, SC05

No.	Topic	Lectures full-time/ part-time	Lab. full-time/ part-time	Self-study full-time/ part-time	Total	Teaching methods	Assessment methods	GC and SC
8	Topic 8. Certification Authorities and a PKI-Based Trust System	4/0.25	2/0.75	9/14	15/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05, SC10
9	Topic 9. Principles of the Theory of Computer Steganography	4/–	2/0.75	9/14	15/14.75	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05, SC10, SC09
10	Topic 10. Steganographic methods for hiding information	2/0.25	4/0.75	9/14	15/15	TM1, TM2	AM1, AM2, AM4, AM7, defense of a laboratory assignment	GC01, SC05, SC09
	Total	**30/2**	**30/10**	**90/138**	**150/150**			

Legend: GC — general competence (number according to section 2); SC — special (professional) competence (number according to section 2). The full wording of each code is given in the educational programme / standard of the specialty.

Teaching methods: TM1 — verbal method (lecture, discussion, interview, etc.); TM2 — practical method (laboratory and practical classes); TM5 — video method combined with up-to-date information technologies and computer-based learning tools (distance, multimedia, web-based, etc.).

Assessment methods: AM1 — exam; AM2 — oral or written survey; AM4 — testing; AM7 — presentation of the results of completed tasks and research.

4. Learning outcomes

PLO19. apply protection theories and methods to ensure information security in information and telecommunication systems;

PLO31. apply protection theories and methods to ensure the security of elements of information and telecommunication systems;

PLO47. address information protection tasks for data processed within information and telecommunication systems, using modern methods and tools for cryptographic information protection;

PLO48. implement and support intrusion detection systems and utilize cryptographic protection components to ensure the required level of information security within information and telecommunication systems;

5. Sustainable Development Goals

SDG 4 – Quality Education

SDG 9 – Industry, Innovation and Infrastructure

SDG 16 – Peace, Justice and Strong Institutions

6. Non-formal education

Recommended courses, training sessions, internships, and similar activities: learning outcomes acquired through formal, non-formal, or informal education may be recognized in accordance with LNTU

procedures. Evidence may include certificates from specialized training sessions, webinars, or online courses, accompanied by a description of the learning outcomes achieved; if necessary, a brief verification task or a portfolio may also be required.

7. Assessment criteria and forms of control

Assessment is based on a 100-point scale (national scale / ECTS). Final grade = continuous assessment (40 %) + module tests (20 %) + exam (40 %).

Academic integrity: independent completion of assignments; correct citation of sources; marking parts of the text generated by AI tools. Violations of academic integrity are not tolerated.

8. Content of topics

Topic 1. Basic Concepts of Cryptology

Key terms: cryptology, cryptography, cryptanalysis, text, encryption, decryption, key, key space, cryptographic system, cryptologic strength, requirements for cryptographic systems. Principles of construction and schemes of cryptologic systems. Classification of encryption algorithms.

Topic 2. General Information on Information Protection in Information and Telecommunication Systems

General information on information protection in information and telecommunication systems. Key objectives of information protection and their significance for the user. The role of cryptographic protocols in the overall task of ensuring information security. General overview of classical cryptology, cryptography, and cryptanalysis.

Topic 3. Fundamentals of C. Shannon's Theory of Secret Communication

Model of an encrypted message transmission system. Perfect cryptographic system. Classification of message encryption methods. Classification of message encryption methods. Cryptanalysis. Classification of cryptanalytic attacks.

Topic 4. Encryption and Public Key Infrastructure

Protection of communications. Methods of protecting devices and hosts in the network infrastructure. Historical examples of text encryption and decryption methods, cryptography methods, as well as physical devices and devices. Encryption using a caesar substitution cipher. Polyalphabetic ciphers. Wigener cipher. Cryptanalysis is code breaking. Use of keys in encryption.

Topic 5. Cryptographic hash functions

Creating a hash code. How a cryptographic hashing algorithm works. Hashing formula. MD5 and SHA. MD5 hashing algorithms. Hash-based Message Authentication Code. Using the HMAC function in Cisco routers.

Topic 6. Encryption

Encryption classes for ensuring data confidentiality. Symmetric encryption. Symmetric encryption algorithms. Classification of encryption algorithms. Asymmetric encryption algorithms. Asymmetric encryption - confidentiality. Asymmetric encryption - authentication. Asymmetric encryption - integrity. Diffie - Hellman algorithm.

Topic 7. Use of digital signatures

Digital signatures. Services provided by digital signatures. Properties of a digital signature. Code digital signatures. Digital signatures for digital certificates.

Topic 8. Certification Authorities and a PKI-Based Trust System

Public key management. Public Key Infrastructure (PKI). PKI center system. PKI-based trust system. Interoperability between different PKI providers. Certificate registration, authentication, and revocation. PKI applications. Encryption of network transactions. Encryption and security monitoring. Encryption and Public Key Infrastructure.

Topic 9. Principles of the Theory of Computer Steganography

General terminological concepts. A generalized model of a steganographic system. Classification of

steganographic systems. Keyless steganographic systems. Steganographic systems with a secret key. Steganographic systems with a public key. Hybrid steganographic systems. Steganalysis. Potential indicators of a steganographic system. Main stages of practical steganalysis. Analysis of the robustness of a steganographic system. Perfectly secure steganographic system. Passive attack: detection of hidden messages. Active and malicious attacks. Robustness of a steganographic system against active attacks. Open steganographic channel.

Topic 10. Steganographic methods for hiding information

Classification of information hiding methods. Text steganography. Methods involving the distortion of a text document's format. Syntactic methods. Semantic methods. Steganogram generation methods. Hiding data in images and video. Substitution methods. Methods for hiding data in the frequency domain of an image. Spread-spectrum methods. Statistical methods. Distortion methods. Structural methods. Hiding information in audio media. Steganographic methods for data protection in audio media.

9. Individual assignments

Not provided for by the curriculum.

10. General requirements

The educational process is governed by the academic regulations of LNTU. Students are required to read the requirements set out in the LNTU Code of Academic Integrity and the LNTU Policy on the Ethical Use of Artificial Intelligence, and to adhere to the principles of academic integrity and the ethical use of artificial intelligence in their educational activities.

Academic integrity. Participants of the educational process must comply with the Law of Ukraine “On Academic Integrity” of 18.12.2025 No. 4742-IX and the internal regulations of LNTU. Academic plagiarism, fabrication, falsification, misappropriation of authorship, non-independent completion of assignments, as well as dishonest use of results generated by artificial intelligence are not allowed.

Use of artificial intelligence. Artificial intelligence tools may be used to search for ideas, explain methods, provide preliminary structuring, language editing and auxiliary analysis of non-confidential data, unless a specific assignment requires fully independent work. Students must indicate the tool used, the purpose and the stage of its use, check facts and calculations, and justify their conclusions independently.

11. References

I. Teaching and methodological materials

Works by other authors:

1. Romadhan, D., & Ferdiansyah, F. (2022). Implementasi Keamanan Database Menggunakan Kriptografi Rc4 Pada Sistem Milik Pt. Torop SumberMakmur. Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia, September, 368–376.

2. Hidayat, M., Tahir, M., Sukriyadi, A., Sulton, A., A, C. A. S., & F, S. A. (2023). Penerapan Kriptografi Caesar Chiper Dalam Pengamanan Data.Jurnal Ilmiah Multidisiplin, 2(03), 35–41.

II. Scientific works

Works by other authors:

3. Joseph D., Misoczki R., Manzano M. et al. Transitioning organizations to post-quantum cryptography. Nature. 2022. Vol. 605, No. 7909. P. 237–243.

4. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization URL: https://doi.org/10.6028/NIST.IR.8413-upd1 (date of application: 23.05.2026).

5. Module-Lattice-Based Digital Signature Standard : FIPS 204. URL: https://doi.org/10.6028/NIST.FIPS.204 (date of application: 23.05.2026).

6. Stateless Hash-Based Digital Signature Standard : FIPS 205. URL: https://doi.org/10.6028/NIST.FIPS.205 (date of application: 23.05.2026).

7. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process : NIST IR 8545. URL: DOI: https://doi.org/10.6028/NIST.IR.8545 (date of application: 23.05.2026).

III. Information resources

8. Cisco. Networking Academy. URL: https://www.netacad.com (date of application: 23.05.2026)