Syllabus
Course Program

Mathematical foundations of cryptology

Specialty
125 – Cybersecurity and information protection

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Cybersecurity

Department
Cybersecurity (328)

Level of education
Bachelor's level

Course type
Special (professional), Mandatory

Semester
3

Language of instruction
English

Lecturers and course developers

Oleksandr MILOV

oleksandr.milov@khpi.edu.ua
Doctor of technical sciences, professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 200 scientific and educational and methodological works. Academic supervisor for protected candidate theses, guarantor of the educational and professional program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Mathematical foundations of cryptology and cryptanalysis", "Data structures", "Industrial and office espionage", "Digital forensics", for undergraduate and graduate students, Section "Methodology of scientific and pedagogical activity in the sciences of cyber protection" for postgraduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Mathematical foundations of cryptology" is a mandatory educational discipline. The study of the discipline provides insight into the main mathematical methods and approaches used to ensure cryptographic protection of information in the process of storing and transmitting information represented in binary codes. The discipline is devoted to the study of the mathematical foundations of cryptology and cryptographic analysis, which are applied to the protection of information in information systems. The discipline reveals the concepts of ciphers, symmetric and asymmetric cryptography, electronic signature, hashing and other mathematical objects of cryptography. The relevant cryptographic standards used today in the protection of information in Ukraine and abroad are studied.

Course objectives and goals

Acquaintance with the mathematical foundations of cryptology; acquisition of skills in practical use, formulation and solving of information encryption problems; understanding the essence of information processes in cryptographic systems; use of computers to solve encryption and decryption tasks;

development and use of mathematical and computational models of information encryption processes, their optimization and development of areas for improvement.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - exam.

Competencies

GC-1. Ability to apply knowledge in practical situations.
GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-3. Ability to abstract thinking, analysis and synthesis.
GC-4. Ability to identify, state and solve problems in a professional manner.
GC-5. Ability to search, process and analyze information.
GC-6. The ability to realize own rights and responsibilities as a member of society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.
PC-1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems.
PC-4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and refusal of various classes and origins.
PC-7. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.).
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-9. Ability to perform professional activities based on the implemented information and/or cyber security management system.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.

Learning outcomes

LOo-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LO-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LO-3. 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. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.

LO-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LOR-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LO-7. Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cyber security.
LO-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LO-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LO-10. Perform analysis and decomposition of information and telecommunication systems.
LO-11. Perform analysis of connections between information processes on remote computer systems.
LO-12. Develop threat and intruder models.
LO-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by hardware and software tools and evaluate the effectiveness of the quality of the decisions made.
LO-15. Use modern hardware and software of information and communication technologies.
LO-16. Implement complex information security systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. Ensure the processes of security and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of security of electronic information resources with a reflection of relationships and information flows, processes for internal and remote components.
LO-18. Use software and software-hardware complexes for the security of information resources.
LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LO-21. Solve tasks of provision and support (including: review, testing, accountability) of the access control system according to the stated security policy in information and telecommunication (automated) systems.
LO-22. Solve the management procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and/or cyber security.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LO-24. Solve the problems of managing access to information resources and processes in information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based).
LO-25. Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and telecommunication (automated) systems using event registration logs, their analysis and stated protection procedures.
LO-26. Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems.
LO-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.
LO-29. Evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means under the conditions of realization of threats of various classes.
LO-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.

LO-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LO-32. Solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the stated security policy.
LO-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LO-34. Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization.
LO-35. Solve the tasks of providing and supporting complex information security systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the stated policy of information and/or cyber security.
LO-36. Detect dangerous signals of technical means.
LO-37. Measure the parameters of dangerous and interfering signals during the instrumental control of information security processes and determine the effectiveness of information security against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system.
LO-38. Interpret the results of special measurements using technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information security system.
LO-39. Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents.
LO–40. 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 security system.
LO-41. Ensure the continuity of the event and incident logging process based on automated procedures.
LO-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LO-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LO-44. Solve the problems of ensuring the continuity of the organization's business processes on the basis of risk management theory and the stated information security management system, in accordance with national and international requirements and standards.
LO-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LO-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LO-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
LO-48. Implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.
LO-49. Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.
LO-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LO-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LO-52. Use tools for monitoring processes in information and telecommunication systems.
LO-53. Solve problems of software code analysis for the presence of possible threats.
LO-54. Be aware of the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 16 hours, laboratory classes - 32 hours, self-study - 72 hours.

Course prerequisites

Mathematical analysis, Linear algebra, Probability theory and mathematical statistics, Discrete mathematics, Informatics, Programming, Legal regulation of cybersecurity.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1. Introduction. Goals and tasks of the educational discipline "Mathematical foundations of cryptology".
The place of discipline in the educational process. The structure and content of the thematic plan for studying the discipline; educational and methodical literature. Peculiarities of studying the discipline; forms of control of students' knowledge, abilities and skills. Directions of scientific research work of students.
Topic 2. Basic concepts of cryptology.
Basic concepts of cryptology and cryptanalysis: cryptographic transformation of information, sender and recipient of information, communication channel, open message, cryptographic key, encryption and decryption processes, cryptogram, cryptographic system, enemy and his attacks. Methods of cryptographic protection of information and the role of cryptography in ensuring information security. The main tasks of cryptography: ensuring the established mode of information access, ensuring the integrity of information, authenticating the author of the message.
Topic 3. Modular arithmetic.
Arithmetic of whole numbers. Set of integers: binary operations, distribution of integers, two constraints, graph of division equation. Divisibility theory. Properties. All divisors. The greatest common denominator. Euclid's algorithm. Extended Euclid algorithm. Linear Diophantine equations. Private solution. General decisions. Modular arithmetic. Modulo operations. System of deductions: Zn. Comparison. System of deductions. Circular notation system. Operations in Zn. Properties. Inversions. Additive inversion. Multiplicative inversion. Addition and multiplication of tables. Different sets for addition and multiplication.
Topic 4. Matrices.
Definition. Operations and equations. Equality. Addition and subtraction. Multiplication. Scalar multiplication. Determinant. Inversions. Additive inversion. Multiplicative inversion. Matrices of deductions. Comparison. Linear equation. Linear equations with one unknown containing comparisons. A system of linear equations containing comparisons.
Topic 5. Simple ciphers.
Categories of simple ciphers. Substitution ciphers. Monoalphabetic ciphers. Additive cipher. Shift cipher. Caesar's Cipher. Multiplicative ciphers. Monoalphabetic substitution cipher. Multi-alphabetic ciphers. Autokey cipher. Playfer cipher. Wigener cipher. Hill's Cipher.
Disposable notebook. Rotary cipher. Enigma machine. The code book is a reference book of ciphers. Permutation ciphers. Permutation ciphers without using a key. Permutation key ciphers. Combining two approaches. Keys. Use of matrices. Ciphers with double permutation.
Topic 6. Algebraic structures.
Groups. Field. Fields GF(2n). Polynomials. Operations. Module. Addition. Multiplication. Multiplication using a computer. Using a generator. Inversions. Additive inversions. Multiplicative inversions. Addition and subtraction. Multiplication and division.
Topic 7. Modern block ciphers.

Substitution, or transposition. Block ciphers as group mathematical permutations.
Full-size key ciphers. Partial-size key ciphers. Ciphers without a key.
Components of a modern block cipher. S-blocks. Cyclic shift. Replacement. Division and union.
Composite ciphers. Dispersion and mixing. Rounds. Two classes of compound ciphers. Feistel network.

Topic 8. DES.

Terms. Structure of DES. Initial and final permutations. Rounds. DES function. Key generation. Remove check bits. Shift to the left. Compression permutation. Analysis of DES. S-blocks. P-blocks. Number of rounds. Weaknesses of DES. Weakness in the cipher key. Multiple use of DES. Double DES. Triple DES. Triple DES with two keys. Triple DES with three keys.

Topic 9. Encryption standard according to GOST 28147-89.

Principles of encryption algorithm construction. The main step and basic cycles of crypto-transformations according to GOST 28147-89. Modes and operation schemes of encryption modes according to GOST 28147-89/

Topic 10. AES cipher.

Criteria. Security. Cost. Realization. Rounds. Data units. Bit. Byte. Word. Bloc. Matrix of states. The structure of each round. Substitution SubBytes. InvSubBytes. Transformation using the GF field. Non-linearity. Permutation. ShiftRows. InvShiftRows. Mix. MixColumns. InvMixColumns. Adding keys. AddRoundKey. Key expansion in AES-128. RotWord. SubWord. RoundConstants. Algorithm. Key extension in AES-192 and AES-256. Key extension analysis.

Topic 11. Cipher "Kalyna -256".

The structure of the encryption algorithm. Modes and operation schemes of encryption modes for "Kalyna -256". Safety and efficiency indicators. Cost. Realization. Rounds.

Topic 12. Simple numbers.

Definition. Mutually prime numbers. The number of prime numbers. The number of prime numbers. The number of prime numbers smaller than n. Check for a prime number. Sieve of Eratosthenes. Euler's phi function. Fermat's Little Theorem. The first version. The second version. Appendices. Euler's theorem. The first version. The second version. Appendices. Generation of prime numbers. Prime Mersenne numbers. Prime Fermat numbers. Testing the simplicity of numbers. Deterministic algorithms. Divisibility theory algorithm. AKS algorithm. Probabilistic algorithms. Fermat's test. The square root test. Miller-Rabin test. Initialization. Recommended number simplicity tests. Factoring. Basic theorem of arithmetic. The greatest common denominator. Least common multiple. Methods of factoring. Distribution verification method. Fermat's method. Pollard's method. Rho - Pollard's method. More effective methods. Quadratic sieve. Sieve field of numbers. Other problems. Chinese remainder theorem.

Topic 13. Quadratic comparison with the module.

Quadratic comparison with the modulus in the form of a prime number. Quadratic subtractions and non-subtractions. Euler's criterion. The solution of the quadratic comparison with the modulus in the form of a prime number. Quadratic comparison by composite modulus. Complexity. Exponentiation and logarithms. Fast promotion. Logarithm. Complete search. Discrete logarithm. Solving the modular logarithm using discrete logarithms.

Topic 14. Cryptographic hash functions.

Message integrity. Hashing functions and data integrity. Requirements for hash functions.
Oracle random model. Iterative hash function (Merkel-Damgard scheme). Message Digest (MD). Secure Hash Algorithm (SHA). Hash functions based on block ciphers (Rabin scheme, Miyaguchi-Prenel scheme. SHA-512. Whirlpool. "Kupina-256" hash algorithm.

Topic 15. Cryptographic system RSA.

Introduction. Keys. General idea. Original text / encrypted text. Encryption / decryption. The need for both cryptosystems. "Loophole" in the unilateral function. Functions. Backpack cryptosystem. Definition. Tuple superincrement. Secret communication with the use of a knapsack. Key generation. Encryption. Decryption. Loophole. RSA cryptographic system. Introduction. Procedure. Two algebraic structures. Key generation. Encryption. Deciphering. Some trivial examples.

Topic 16. Cryptosystems of Rabin and El-Gamal. Diffie-Hellman algorithm.

Procedure. Key generation. Encryption. Deciphering. The security of Rabin's cryptographic system. The cryptographic system of El-Gamal. Procedure. Key generation. Encryption. Deciphering. Security analysis of the El-Gamal cryptosystem. Small module attacks. Attack of knowledge of the source text. Diffie-Hellman algorithm.

Topic 17. Cryptosystems based on the elliptic curve method.

The equation of the elliptic curve. Singular and non-singular curves. Operations with points. The use of elliptic curves in cryptography. Elliptic curves in real numbers. Abelian group. Group and field. Elliptic curves in GF(p). Finding the inversion. Finding points on a curve. Addition of two points. Multiplying a point by a constant. Elliptic curves in GF. Elliptic curve cryptography modeling the El-Gamal cryptosystem. Generation of public and private keys. Encryption. Deciphering. Comparison. Safety of the elliptic curve method. Module size.

Topic 18. Digital signature.

Digital signature concept. Digital signature process. Security services provided with a digital signature. Digital signature attacks. Digital signature schemes (RSA, El-Gamal, Shnora, DSS, elliptic curve). Digital signature programs.

Topic 19. Pseudorandom numbers in cryptography.

Advantages and prospects of using stream encryption systems. Use of random numbers (randomness, unpredictability). Sources of random numbers. Pseudorandom number generators: round-robin encryption, post-exit feedback mode, ANSI X9.17 pseudorandom number generator, BBS generator, linear congruent method, delayed Fibonacci method. Checking the quality of the pseudorandom number generator. Sequences of maximum length. Analysis of pseudorandom sequences.

Topic 20. Cryptoanalysis.

Kerckhoffs principles. Cryptoanalysis. Common cryptanalysis methods: brute force, space-time trade-offs, rainbow tables, slide attacks, cryptanalysis of hash functions, cryptanalysis of random number generators. Linear cryptanalysis. General overview. Matsui's algorithms. Linear expressions for S-boxes. Matsui's Lemma on Accumulation. Easy1 cipher Linear expressions and key recovery. Linear DES cryptanalysis. Multiple linear approximations. Finding linear expressions. Linear cryptanalysis code. Differential cryptanalysis. General overview. Marking. S-Box differentials. A combination of S-Box characteristics. Output of the key. Differential cryptanalysis code. Differential cryptanalysis of Feistel ciphers. Differential linear cryptanalysis. Conditional characteristics. Differentials of higher order. Truncated differentials. Differentials are impossible. Boomerang attack. Interpolation attack. Linked Key Attack.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Acquaintance with the envelope of performing laboratory work in cryptology. Information preparation tools for laboratory work.

Topic 2. Research of modern block symmetric ciphers and encryption modes.

Topic 3. Encryption and decryption in substitution and permutation ciphers. Encryption and decryption in Enigma rotary machines.

Topic 4. Research of modern block symmetric ciphers and encryption modes. Study of modern asymmetric encryption cryptosystems.

Topic 5. Performing cryptographic transformations in DES. Key generation in DES.

Topic 6. Performing cryptographic transformations in AES. Key generation in AES.

Topic 7. Generation and research of hash functions.

Topic 8. Generation of keys in the RSA system. Encryption and decryption. Use and study of Rabin, El-Gamal and Diffie-Hellman algorithm cryptosystems.

Self-study

A student's independent work is one of the forms of organization of learning, the main form of mastering educational material in free time from classroom training. During independent work, students study lecture material, do individual homework, prepare for tests, tests and exams. Students are also recommended additional materials (videos, articles) for self-study and analysis.

Non-formal education

Within the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the

case of independent completion of professional courses/trainings, civic education, online education, vocational training, etc.
Subjects are not considered for this component in case of successful completion of the courses.

Course materials and recommended reading

Basic literature:

1. Yevseev S.P. Cybersecurity: Cryptography with Python: a tutorial. - Lviv "New World-2000", 2021. - 120 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
2. Yevseev S.P. Cybersecurity: Laboratory workshop on the basics of cryptographic protection. - Lviv "New World-2000", 2020. - 241 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. Yevseev S.P. Cyber security: modern protection technologies. / Yevseev S. P., Ostapov S. E., Korol O. G. // Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678 p.
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
4. Information protection technologies./ S. E. Ostapov, S. P. Yevseev, O. G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
5. Yevseev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. - 657 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Additional literature:

6. Yevseev S.P. Cyber security: Laboratory workshop on the basics of cryptographic protection. - Lviv "New World-2000", 2020. - 241 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Bobalo Y. Ya., Gorbaty I. V. (eds.) Information security. Study guide. – Lviv: Publishing House of Lviv Polytechnic, 2019. – 580 p. - ISBN 978-966-941-339-0
http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
8. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Points are awarded according to the following ratio:
- laboratory work: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- exam: 40% of the semester grade.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic integrity and course policy

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU "KhPI": to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed in academic groups with a lecturer, and if it is impossible to resolve the conflict, they should be brought to the attention of the Institute's management.
Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU "KhPI" are available on the website: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV