Syllabus
Course Program

Decentralised systems

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
Profile training, Selective

Semester
4

Language of instruction
English

Lecturers and course developers

Serhii YEVSEIEV

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

The number of scientific publications: more than 350, including 42 utility model patents, 17 monographs, of which 9 are collective monographs, 31 textbooks, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 163 articles in foreign publications and specialized publications of Ukraine, with 61 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management", "Introduction to networks", "Security of banking systems", "Hybrid warfare and national security", "Audit and monitoring of corporate networks", "Blockchain: basics and application examples", "Fundamentals of smart contracts", "Basics of cyber security" for undergraduate and graduate students, Section "Methods and technologies of information security monitoring and auditing", "Methods of building post-quantum cryptosystems", "Latest technologies for ensuring cyber security based on blockchain technology" for postgraduate students.

More about the lecturer on the department's website

Roman KOROLEV

roman.korolev@khpi.edu.ua
Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 80, including 12 utility model patents, 1 collective monograph, 2 training manuals, 65 articles in foreign publications and specialized publications of Ukraine, 5 of them in the Scopus scientometric database. Leading lecturer in the disciplines: "Wireless and mobile security", "Fundamentals of steganography", "Business intelligence",

"Physical foundations of technical means of intelligence" for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

he study discipline "Decentralized systems" is a selective study discipline. The subject of study of the academic discipline is theoretical concepts, principles of operation, development and application to complex decentralized technologies, principles of forming mesh networks.

Course objectives and goals

Mastering the theoretical foundations and obtaining practical skills in the use of decentralized technologies, the principles of forming mesh networks.

Format of classes

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

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
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-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
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

LO-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.
LO-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 90 hours (3 ECTS credits): lectures - 16 hours, laboratory classes - 16 hours, self-study - 58 hours.

Course prerequisites

Computer networks, Integrated information security systems, Security in information and communication systems, Fundamentals of mathematical modelling of security systems.

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. Decentralization in information systems.
Concept of decentralization for information systems. Decentralized file sharing systems. Application of the principles of decentralization. Typical architecture of decentralized systems. Advantages and limitations of decentralized systems.
Topic 2. Decentralization as an approach in information systems.
Peer-to-peer networks and the BitTorren protocol. Principles of building a peer-to-peer file sharing network. Principle of operation and application of Distributed Hash Table. Web-of-trust concept. Principles of operation of web-of-trust, BitMessage, IPFS. Filecoin Consensus Algorithm.
Topic 3. Cryptography in decentralized systems.
Generation and processing of key data. Principles of key generation. Generators of random sequences. Generators of pseudorandom sequences. Key Generation Functions (KDF). Key exchange protocols. Diffie-Hellman protocol on elliptic curves. EKE protocol. Concept and application of Merkle Tree. Types of digital signatures. Lamport one time signature. Winternitz one time signature. Multi-signature Threshold signature. Group signature. Ring signature. Blind signature.
Topic 4. Bitcoin as a platform.
One-way peg and two-way peg sidechains. Lightning Network Device. Penalty mechanism for fraud in the channel. Principles of operation and application of atomic swap. Application of atomic swaps by decentralized exchanges. Proof-of-stake algorithms for achieving consensus. The main disadvantages and risks of using proof-of-stake.
Topic 5. Methods of ensuring confidentiality in modern accounting systems.
CryptoNote standards. MimbleWimble transaction model.Principles of homomorphic encryption. Quadratic Arithmetic Programs.
Topic 6. Development of decentralized technologies.
Setting up the Bitshares protocol. Decentralized asset exchange. SmartCoins. Database organization. Optimizing the execution of business logic.
Topic 7. Application of decentralized approaches to the organization of various systems.
Principles of mesh network operation and development. Popular protocols for organizing mesh networks. Decentralized systems of digital identification. OpenID and OpenID Connect protocols. Expanding the capabilities of the global identification system using blockchain technology.
Topic 8. Decentralized electronic voting platforms.
Decentralized approach to electronic voting. Using blockchain technology for the electronic voting system.
Topic 9. Technologies of decentralized exchanges.
Principles of functioning of decentralized exchanges. Escrow. Atomic Swap. 0x Protocol. Internal exchanges.
Topic 10. Decentralized auction.
The principle of the online auction. The principle of operation of the decentralized online auction.
Topic 11. Using the concepts of sharding, off-chain and dag for scaling accounting systems.
Use of off-chain protocols. Sharding in blockchain-based systems. Exchange messages between shardchains. Construction and application of Directed acyclic graph Architecture of distributed accounting systems based on DAG.
Topic 12. Features and role of cryptographic obligations in accounting systems.
Features and methods of construction of cryptographic obligations. Pedersen Commitment. Knowledge exchange and Nothing Up My Sleeve approaches.ElGamal commitment scheme. The Schnorr Identification Protocol as an interactive zero-disclosure proof scheme. Schnorr's identification scheme. Using the Pedersen Commitment for Zero Disclosure Evidence. Use of Pedersen Commitments in Confidential Transaction. Signature algorithms that are based on the use of hash functions. HORS design. Merkel's signature scheme. The Sphincs family of algorithms.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Basic configuration of Kali Linux and Metasploitable 2.
Topic 2: Using Google for OSINT in penetration testing projects. Technical intelligence of IT infrastructure. Using Maltese for Intelligence.
Topic 3. Vulnerability analysis Port scanning. Manual vulnerability assessment. Using vulnerability scanners to assess vulnerabilities. Configuration overview. Special scanning tools.
Topic 4. Exploitation Attack using ARP spoofing. Using the Metasploit command line to exploit vulnerabilities. Using Armitage to exploit vulnerabilities. Attacks on database passwords. Attacks on passwords for various services.
Topic 5. Operation of web applications Scanning of web applications. Choosing a web application password. Executing OS commands through a web server.
Topic 6. Operation of web applications. SQL injection and offline password cracking. Exploitation of XSS vulnerability.
Topic 7. Exploitation Using Client Attacks Client Exploitation with BeEF.
Topic 8. Access support Installation and use of rootkits.

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. Kravchenko P. Blockchain and decentralized systems. Part 1 – Kharkiv: PROMART, 2019. – 452 p. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0e26ed5b-990d-4271-85f8-573434a7722f/content
2. Kravchenko P. Blockchain and decentralized systems. Part 3 - Kharkiv: PROMART, 2020. - 306 p.
3. Synergy of building cybersecurity systems: monograph / S. Yevseiev, 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
4. 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
5. 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.

Additional literature:

6. Dragoslav D Siljak, Decentralized Control of Complex Systems, 2012. https://www.abebooks.com/9780486486147/Decentralized-Control-Complex-Systems-Dover-0486486141/plp
7. Arthur G.O. Mutambara. Decentralized Estimation and Control for Multisensor Systems, 2019.

https://www.perlego.com/book/1493337/decentralized-estimation-and-control-for-multisensor-systems-pdf
8. Anuj Bhatia. Centralized vs Decentralized Air-conditioning Systems: Quick Book, 2015. https://www.cedengineering.com/userfiles/M05-012%20-%20Centralized%20Vs.%20Decentralized%20Air%20Conditioning%20Systems%20-%20US.pdf.

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