Syllabus
Course Program

Security of banking 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, Selective

Semester
6

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

Olha KOROL

olha.korol@khpi.edu.ua
Candidate of technical sciences, associate professor, associate professor of the department of cyber security of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 150, of which 14 are textbooks, 48 articles in foreign publications and specialized publications of Ukraine, 8 patents for a useful model, 9 in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management", "State national security", "State information security", "Comprehensive training "Security of web applications"" for undergraduate and graduate

students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Security of banking systems" is an optional educational discipline. In modern conditions, as practice has shown, an important role in ensuring the national security of Ukraine and especially its economic component belongs to the processes of ensuring the state's information security (IS) in the banking sector (BnS). A key role in the construction of security systems of banking information resources (BIR) as components of the national information resources of the state is played by theory and practice, in which the scientific and methodological base is the basis for making reasonable and effective management decisions by subjects of state IS provision at all levels.

Course objectives and goals

Mastering by students a set of knowledge in the field of protection of banking information resources, systems and methods of determining the security of software products in automated banking systems, acquiring, on the basis of this knowledge, practical skills and theoretical knowledge necessary for a creative approach to the issue of modern and in the future operational protection of the contour of business processes in banking sector organizations. Formation of professional competence of future cyber security specialists, sufficient for work as a bank information security administrator and necessary for career development.

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 120 hours (4 ECTS credits): lectures - 24 hours, laboratory classes - 24 hours, self-study - 72 hours.

Course prerequisites

Fundamentals of cryptographic protection, Fundamentals of construction and protection of modern operating systems, Complex information protection 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. The structure of the internal payment system of a commercial bank. Security services and mechanisms.
The main components of information security of the state. Regulations. Basic principles and mechanisms of ensuring information security in banking systems of Ukraine. Basic functions of banking systems. Structural diagram.
Topic 2. Legal provision of banking security.
Recommendations of international standards. Resolution of the NBU dated September 28, 2017 No. 95. Group and partial indicators of IS. The concept of building a synergistic threat model. Standard SOU N NBU 65.1 SUIB 1.0: 2010. Information security management system.
Topic 3. Access to banking information.
Basic banking information resources. Trust policies. Security infrastructure concept. The purpose and services of the security infrastructure. Authentication mechanisms.
Topic 4. Risks in banking activity.
Classification of cyber attacks on banking systems. Statistics of targeted attacks 2020-2021. A synergistic model of BIR security threats. An improved model of the attacker.
Topic 5. Public key certificates. The PGP system.
The main mechanisms of public key technology and PGP in automated banking systems. Certification protocols.
Topic 6. Risk assessment in banking.
Information security audit. Methods of risk assessment.
Topic 7. Security of microprocessor cards.
Internal payment system of a commercial bank. Plastic card standards. Validity security mechanisms. Smart cards. Contact and contactless smart cards. Operating systems of smart cards. 3D Secure.
Topic 8. Electronic data exchange systems.
Advantages of ISMS implementation. Objectives and result of ISO27001 implementation. Description of critical business processes and software and technical complexes that ensure their functioning. Bank network structure. Principles of ensuring continuity of work. Risk assessment methodology. Implementation and functioning of ISMS.
Topic 9. Technology of protection of interbank payments. First Virtual payment system: security without encryption.
EDI systems. EDIFACT system. Security of EDI systems. First Virtual payment system: security without encryption.
Topic 10. Actual problems of information and cyber security in the banking sector.
Legal basis. Use of cloud technologies. Methods of spreading pests. ATM attacks. Harmful samples. Theft through ATM Switch.
Topic 11. Digital currencies. cryptocurrencies.
Organization of BITCOIN transaction. The concept of BLOCKCHAIN. Mining main stages. Models and mechanisms of obtaining consensus. Basics of smart contract protocols.

Topic 12. Protected protocols.
SSL protocol in banking systems. Alert protocol. SET protocol. OAER technology.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Study of GnuPG and Kleopatra information protection system.
Topic 2. Study of data protection system VeraCrypt 1.24.
Topic 3. Study of the KryptoBank 5.0 data protection system.
Topic 4. Research on information protection in simplified EDI systems.
Topic 5. Development of the ATM system.
Topic 6. Study of message protection in the SET protocol.

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. On the protection of information in information and telecommunication systems: Law of Ukraine dated 07.05.1994 No. 80/94-VR. Update date: 12/31/2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI. Date of update: 10/27/2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Decree of the President of Ukraine: On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine dated May 6, 2015 No. 287/2015. Date of update: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
4. On national security: Law of Ukraine dated June 21, 2018 No. 2469-VIII. Date of update: 03/31/2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. Decree of the President of Ukraine: On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine" No. 96/2016. Update date: 08/28/2021. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
6. Regulation on technical protection of information in Ukraine, approved by the Decree of the President of Ukraine dated 09/27/99 No. 1229. Date of update: 05/04/2008. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text
7. DSTU 3396 0-96 Information protection. Technical protection of information. Basic provisions. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
8. DSTU 3396 1-96 Information protection. Technical protection of information. The order of work. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
9. ND TZI 1.1-003-99 Terminology in the field of information protection in computer systems against unauthorized access. Approved by the order of the DSTSZI of the Security Council of Ukraine dated 04.28.99. No. 22.

https://tzi.ua/assets/files/1.1_003_99.pdf
10. ND TZI 2.5-004-99 Criteria for evaluating the security of information in computer systems against unauthorized access, order of the DSTSZI of the SBU dated 04.28.99 No. 22 (Amendment No. 1 order dated 12.28.2012 No. 806).
https://tzi.com.ua/downloads/2.5-004-99.pdf
11. ND TZI 1.1-002-99 General Provisions on Protection of Information in Computer Systems from Unauthorized Access, Order of the DSTSZI of the SBU dated 04/28/99 (Amendment No. 1 Order of the State Special Communications Administration dated 12/28/2012 No. 806).
https://tzi.com.ua/downloads/1.1-002-99.pdf
12. ND TZI 1.1-005-07 Protection of information at objects of information activity. Creation of a complex of technical protection of information. Basic provisions.
https://tzi.com.ua/downloads/1.1-005-07.pdf
13. ND TZI 1.4-001-2000 Standard provision on the information protection service in automated systems, order of the DSTSZI of the SBU dated 04.12.2000 No. 53 (Amendment No. 1 order of the State Special Communications Administration dated 28.12.2012 No. 806).
https://tzi.com.ua/downloads/1.4-001-2000.pdf
14. Cyber security: modern protection technologies. Study guide for students of higher educational institutions. / S.E. Ostapov, S.P. Yevseev, O.G. King. – Lviv: "New World-2000", 2020. - 678 p.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
15. 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:

16. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html
17. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
18. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html.
19. 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
20. Kravchenko P. Blockchain and decentralized systems. Part 3 - Kharkiv: PROMART, 2020. - 306 p.
21. Yevseyev S.P. CYBER SECURITY: LABORATORY PRACTICUM ON THE FUNDAMENTALS OF CRYPTOGRAPHIC PROTECTION / S.P. Yevseev, O.V. Milov, O.G. Korol - Lviv: "New World-2000", 2020. - 241 p.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.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