Syllabus
Course Program

Protecting critical infrastructure facilities

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
7

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

Alla HAVRYLOVA

alla.havrylova@khpi.edu.ua
PhD, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 30, including 2 utility model patents, 3 monographs, of which 1 is in a peer-reviewed edition included in the Scopus database, 1 is in a foreign scientific publication, 2 is in a specialized publication of Ukraine; 14 articles, of which 7 scientific articles are in Ukrainian scientific publications, 4 scientific articles are in peer-reviewed publications included in the Scopus database, 3 articles are in foreign scientific publications. Lecturer on disciplines: "Introduction to the specialty. Introductory practice",

"Organizational provision of information protection" for undergraduate students
More about the lecturer on the department's website

Andrii TKACHOV

andrii.tkachov@khpi.edu.ua
Candidate of Technical Sciences, senior researcher of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 60 publications, 25 articles in foreign publications and specialized publications of Ukraine, 6 patents for a useful model, guarantor of the educational and professional program of the first (bachelor) level of higher education. Leading lecturer in the disciplines: "Network Programming", "Development and Analysis of Algorithms", "Programming Technologies", "Programming Tools", "Web Security", "Fundamentals of Technical Information Protection", for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Protecting critical infrastructure facilities" is a selective educational discipline. The study of the discipline is aimed at determining the information that needs protection at critical infrastructure facilities (CIF). Mastering methods and means of technical information protection at CIF. Familiarization with information leakage channels and the reasons for their formation. Mastering the skills of working with the means and complexes of detection of embedded devices of unauthorized obtaining of information. Mastering the skills of working with the means and complexes of information protection at OKI. Mastering the procedure for the examination and analysis of CIF in order to ensure the protection of information. Mastery of organizational and technical measures for information protection at CIF.

Course objectives and goals

Teaching students the principles of determining general requirements for cyber protection of critical infrastructure objects, establishing a list of basic cyber protection measures that must be implemented at a critical infrastructure object, based on the requirements of international information security standards, state regulatory documents on information protection technology, determining procedure and criteria for classifying objects as critical infrastructure objects.

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

Higher mathematics, Mathematical foundations of cryptology, Integrated information 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. General requirements for cyber protection of critical infrastructure objects.
List of basic requirements for ensuring cyber protection of critical infrastructure objects.
Topic 2. Physical protection of critical infrastructure objects.
Stories of battles. Hackers. Impact of threats. State-of-the-art Security Monitoring and Control Center (SOC). Protection of infrastructure communications.
Topic 3. Cyber protection of infrastructure.
Major cyber threats to critical infrastructure. Criminals and their tools.
Topic 4. Management of crisis situations and elimination of consequences.
How to organize effective management of crisis situations in critical infrastructure. Implementation of the concept on the example of ABS of Ukraine. Threat classifier. Improved ABS infrastructure model. Conceptual and synergistic models of security. Improvement of the security level assessment model. Coordination of actions of various agents during a crisis situation.
Topic 5. Protection of telecommunication infrastructure.
How to protect telecommunications networks from cyber attacks. Network segmentation and microsegmentation. Monitoring and centralized management. Next Generation Firewall (NGFW). Unified threat management (UTM). Inspection of encrypted traffic. Protection against leakage of confidential information. Implementation of two-factor authentication solutions. Combining local networks and remote access.
Topic 6 Protection of electric power infrastructure.
Threats and vulnerabilities for electric power infrastructure. Attacks on IoT infrastructure. Strategies and technologies for the protection of electric power infrastructure.Challenges facing international cooperation in the field of energy infrastructure protection.
Topic 7. Protection of financial infrastructure.

The main threats and risks to the financial infrastructure, tools for their detection and assessment. Methods and technologies for protecting financial transactions and data in banks and financial institutions. Standards and regulatory requirements to ensure the security of financial infrastructure. Current trends and innovations in cyber security to protect financial systems and infrastructure.
Topic 8. International cooperation in the protection of critical infrastructure.
International organizations and initiatives for the coordination of measures for the protection of critical infrastructure between countries. International agreements and mechanisms of cooperation to ensure the safety of critical infrastructure. Green book on critical infrastructure protection in Ukraine. Sectors, objects, systems that can be classified as critical infrastructure. The main threats to critical infrastructure. State policy of protection of critical infrastructure. Strategic goals of the state policy of critical infrastructure protection. Basic principles of formation of protection of critical infrastructure in Ukraine. Critical infrastructure protection system in Ukraine. Development of mechanisms for the protection of critical infrastructure in Ukraine.
Topic 9. Conditions for the emergence of a terrorist threat and countermeasures.
Analysis of the essence and content of the problem of information security of the state at the current stage of the development of science and technology. Factors of origin of terrorism. Options for the classification of terrorism. Types of terrorists. Motives of terrorists. Methods of increasing the level of cyber protection of a critical information structure.
Topic 10. Instrumental means of information security risk management of critical infrastructure objects.
Information security risk management tools/ Risk assessment models of the company Digital Securit. Threat and vulnerability analysis model. Principle of operation of the algorithm. Calculation of risks for threats to information security. Task of countermeasures. Payment infrastructure.
Topic 11. Management system as an object of cyber security.
Analysis of the management system as an object of cyber security. Features of the analysis. Basics of detection and search of objects with critical cybernetic infrastructure.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Study of general requirements for cyber protection of critical infrastructure objects.
Topic 2. Critical infrastructure by region of Ukraine. Organizational principles of the region of Ukraine as components of the national system of critical infrastructure protection.
Topic 3. Compilation of information about the object of critical information infrastructure of the specified region of Ukraine.
Topic 4. Study of the features of the national critical infrastructure protection system.
Topic 5. Study of the peculiarities of the formation of Technical requirements for the creation of specialized software "State register of objects of critical information infrastructure".
Topic 6. Study of measures to ensure cyber protection of critical information infrastructure of banks.
Topic 7. Methodological recommendations for the development of the current and target profile of cyber protection. Methodological recommendations for the analysis of the current and target profile of cyber protection.
Topic 8. Carrying out the classification of cyber protection measures of critical infrastructure objects.

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.

In particular, certain topics of this component can be taken into account in case of successful completion of the following CISCO courses:
CyberOps
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. On critical infrastructure: Law of Ukraine dated November 16, 2021 No. 1882-IX. Date of update: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. On the approval of General requirements for cyber protection of critical infrastructure objects: Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019 No. 518. Date of update: 09/07/2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
3. Some issues of critical information infrastructure objects: Resolution of the Cabinet of Ministers of Ukraine of October 9, 2020 No. 943. Date of update: 09/07/2022. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
4. Methodological recommendations for increasing the level of cyber protection of critical information infrastructure. Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated October 6, 2021 No. 601. https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
5. On the approval of forms for submitting information to the state register of objects of critical information infrastructure: Order of the State Special Communications Administration dated September 2, 2023 No. 793 https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru-ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veresnya-2023-roku-793
6. On the approval of the Regulation on the organization of cyber protection in the banking system of Ukraine: Resolution of the Board of the National Bank of Ukraine dated August 12, 2022 No. 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
8. Information protection technologies./ S.E. Ostapov, S.P. Yevseev, O.G. King.– Chernivtsi: Chernivtsi National University, 2013. – 471 p. http://kist.ntu.edu.ua/textPhD/tzi.pdf
9. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. http://monograph.com.ua/pctc/catalog/view/64/52/231-1
10. 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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
11. 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. http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Additional literature:

12. 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
13. 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
14. 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.

Assessment and grading

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

Points are awarded according to the following ratio:
- laboratory work: 30% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 20% 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