Syllabus
Course Program

Risk management

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

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 study discipline "Risk Management" is a selective study discipline. The discipline is aimed at the formation of professional competences in the identification, assessment and management of risks in the process of assimilation of theoretical and practical aspects of risk management.

Course objectives and goals

Acquisition by future specialists of competencies that ensure effective risk management in modern cyber systems, enable a qualified assessment of risks in conditions of widespread use of modern cyber security methods.

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, Management of information security, 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. Basic concepts and definitions in the field of cyber security.
Basic concepts. Classification of risks. Signs of risks. General scheme of the risk management process. Stages of risk management. Risk assessment. Threat assessment and management. Microsoft security risks.
Topic 2. Prediction of cyber threats.
Malicious software. Typical network attacks are Intelligence, Access and Social Engineering. Network Attacks – Denial of Service, Buffer Overflow and Evasion. Who is attacking our network? Hackers' tools.
Topic 3. Identification of information systems assets.
Identification of information resources. Software identification. Identification of users and roles. Assessing the importance of assets. Asset life cycle management. Network monitoring and monitoring tools. General information about network monitoring tools.
Topic 4. Management of crisis situations and elimination of consequences.
Effective management of crisis situations in critical infrastructure. Implementation of the concept on the example of OBS of Ukraine. Threat classifier. Security models. Improvement of the security level assessment model. Classification of intruders. Coordination of actions of various agents during a crisis situation.
Topic 5. Crisis management.
The essence of the concept of "crisis". Functions of the anti-crisis management system. Signs of a crisis in an economic phenomenon. Consequences of the crisis. Phases of the crisis. The essence of the factors. Classification of crisis phenomena. Structural diagram of the process of forming an anti-crisis program. The main tasks of the crisis management manager.
Topic 6. Internal and external threats. Using_IDS_and_IPS.
Key criteria for classifying cyber incidents. IP vulnerabilities. TCP and UDP vulnerabilities. IP services. Corporate services. Intrusion detection and prevention systems. Methods of system monitoring. Analysis of intrusion detection methods. Evaluation of notifications Security Onion. Well-known intrusion detection and prevention systems. Comparative analysis of modern intrusion detection and prevention systems.
Topic 7. Approaches to building a threat and offender model.
The mechanism of destructive influence on the information system. Model of information security violator. The main channels of information leakage. Offended insiders. Disloyal insiders. Classification of insiders according to the criterion of motivation. Method of implementation of the attack (at the place of action).
Topic 8. Policy of the management system.
Information security management system. Approximate sequence of actions in the development of SMIB. An example of an information security policy. Examples of failed policies. Cybersecurity cost analysis. Development of the budget.
Topic 9. Analysis of logs: collection, aggregation, interpretation.
Tools for collecting log data from various network components and systems. Methods for aggregating log files from different sources into one centralized repository. Normalization of log data to ensure a standard format and facilitate their further analysis. Techniques and algorithms for detecting anomalies in logs that may indicate cyber threats or other problems. Network and server profiling. Common Vulnerability Assessment System (CVSS).
Secure device management.
Topic 10. Management of information security incidents.
Relationship of concepts. Qualitative evaluation of SMIB.Content of the incident management process. Causes of incidents. Incident Investigation Team. The structure of the information security incident

investigation team. Development of regulatory documents on incident management. Detection and analysis of information security incidents. Documenting an information security incident. Prevention of the spread of the incident. Identification of the offender. Storage of materials. Checklists of observations.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Installing the CyberOps Workstation virtual machine.
Cyber security: practical examples. Studying information about the attack. Visualization of "black" hackers. How to become a defender.
Topic 2 Study of processes, threads, descriptors and the Windows registry.
Creating user accounts. Using Windows PowerShell. Windows Task Manager. Monitoring and managing system resources in Windows.
Topic 3. Route tracking. Getting to know Wireshark.
Using Wireshark to examine Ethernet frames. Using Wireshark to observe a three-way TCP handshake. Using Wireshark to examine captured UDP DNS messages. Using Wireshark to examine TCP and UDP captured packets. Using Wireshark to examine HTTP and HTTPS traffic. Study of DNS traffic. An attack on the MySQL database. Using Wireshark to examine HTTP and HTTPS traffic. Study of DNS traffic. An attack on the MySQL database.
Topic 4. Using Wireshark to examine Ethernet frames.

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:
Cyber Threat Management
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. Ozkaya, Erdal. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Packt Publishing Ltd, 2018.- 557 p.
https://h.twirpx.link/file/2523887/
2. Alexander, Michael; Wanner, R. Methods for understanding and reducing social engineering attacks. SANS Inst., 2016, 1: 1-32.
https://www.giac.org/paper/gccc/270/methods-understanding-reducing-social-engineering-attacks/147205
3. Hadnagy, Christopher. Social engineering: The science of human hacking. John Wiley & Sons, 2018 - 330 p.
http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf
4. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective measures of Ethical Hacking Paperback – July 23, 2020 – 456 p.

https://books.google.com.ua/books/about/Ethical_Hacking.html?id=7D3AzQEACAAJ&redir_esc=y
5. Buryachok V. L. Information and cyber security: socio-technical aspect: textbook / [V. L. Buryachok, V. B. Tolubko, V. O. Khoroshko, S. V. Tolyupa]; in general ed. Dr. Tech. of Sciences, by Professor V. B. Tolubka. – K.: DUT, 2015. – 288 p.
https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf
6. 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.
7. 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.
8. 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.

Additional literature:

1. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model. URL:
https://www.iso.org/search.html?q=15408-1.
2. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL:
https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
3. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components. URL:
https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
4. ISO/IEC 31010:2019 Risk management . URL:
https://www.iso.org/ru/contents/data/standard/07/21/72140.html
5. 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
6. 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
7. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance URL:
https://www.iso.org/ru/contents/data/standard/06/34/63417.html
8. 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
9. ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security. URL:
https://www.iso.org/ru/contents/data/standard/07/60/76070.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

28.08.2023 — Head of the department
Serhii YEVSEIEV

28.08.2023 — Guarantor of the educational program
Serhii YEVSEIEV