Syllabus

Course Program

Risk theory in cybersecurity

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 5	Language of instruction English

Lecturers and course developers

Oleksandr MILOV

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

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

General information

Summary

The educational discipline "Theory of risks in cyber security" is aimed at the fact that students acquire theoretical knowledge about the formation and development of the theory and practice of risk analysis and management, conceptual apparatus and terminology, regarding risk-creating factors, structures and models of risks, practical skills in defining and performing tasks regarding timely detection, assessment and analysis of risks, in each specific case, the ability to perform the task of risk management, knowledge of the requirements of international and domestic standards in this area, knowledge of mathematical methods and tools that are used for risk assessment and analysis and make risk management more effective Acquired knowledge and skills can be used by students in their future professional activities.

Course objectives and goals

The purpose of the educational discipline "The theory of risks in cyber security" is to provide an idea of the essence and content of the concept of "risk", types and models of risks, their classification, defining properties and ways of formation, methods of risk analysis and forecasting, as well as the main principles of management risks in various spheres of human activity.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control – credit test.

Competencies

GC-1. Ability to apply knowledge in practical situations.
GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-3. Ability to communicate professionally in both spoken and written national and foreign languages.
GC-4. Ability to identify, state and solve problems in a professional manner.
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-3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems.
PC-4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.

Learning outcomes

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-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 - 32 hours, laboratory classes - 16 hours, self-study - 72 hours.

Course prerequisites

"Probability theory" and "Mathematical statistics".

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 essence of risk.
Risks in the historical aspect and in the modern world. Main characteristics of risks. Peculiarities of the development of risk theory in various areas.
Topic 2. Mechanisms of occurrence and development of risks.
Uncertainty and its features. Structure of risks. Models (concepts) of risks. Risk assessment problems in the "uncertainty-risk" model.
Topic 3. Dangers, threats and vulnerabilities of risk objects, types, characteristics, classification.
Risk analysis: analysis concepts, types and tasks, analysis methods.
Topic 4. Methods and features of risk assessment.
Forecasting risks and losses from their implementation. Peculiarities of expert analysis and risk assessment.
Topic 5. Risk management organization, risk management process.
Risk management methods in cyber security. Security incident management.
Topic 6. Peculiarities of decision-making on the management of certain specific types of risks.
Psychological aspects of decision-making in conditions of risk. Risk communication.
Topic 7. Peculiarities of entrepreneurial and economic risks.

Individual risks: assessment of risks of premature death, acceptability of individual risk, regulation of individual risk.

Topic 8. Information risks.

Evaluation methods. A value-motivational approach to the analysis of information risks.

Topic 9. International standards on risk management.

ISO standards on the principles of information risk analysis and management. National regulatory support for risk management.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. General algorithm of complex risk assessment.
Topic 2. Calculation and assessment of risk and average risk. Calculation and construction of a risk profile.
Topic 3. Justification of the choice of risk models for typical situations of threat realization
Topic 4. Processing of group examination results, evaluation of expert competence levels and quality of expert group selection
Topic 5. Building a model of expert competence, processing the results of a group examination involving model evaluations of expert competence.
Topic 6. Development of provisions on internal control and risk management
Topic 7. Assessment of the economic risks of choosing an information protection system option under the conditions of known probabilities of threats and corresponding losses.
Topic 8. Assessment of the risks of human death from various factors and causes and individual risks of death and becoming a victim of an accident of a resident of a certain settlement
Topic 9. Calculation of the overall risk of the possible realization of a threat to information resources that belong to the assets of the corporate information system under the conditions of known damage from a violation of the confidentiality of the resource.

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

References

1. Borovyk M.V. Risk management: lecture notes / Borovyk M.V.; Kharkiv. national city university farm named after O. M. Beketova. – Kharkiv: XNUMX named after O. M. Beketova, 2018. – 65 p. URL: https://eprints.kname.edu.ua/62534/1/%D0%91%D0%BE%D1%80%D0%BE%D0%B2%D0%B8%D0%BA%2C%20151 %D0%9B%2C%202022%2C%20pdf.pdf
2. Danyk Y.G. Fundamentals of cyber security and cyber defense: textbook / Yu.G. Danyk, P.P. Vorobienko, V.M. Chernega, second edition, revised, supplemented - Odesa: ONAZ named after O.S. Popova, 2020. – 327 p. URL: https://kr-labs.com.ua/books/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8+%D1%82%D0%B0+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%BE%D0%B1%D0%BE%D1%80%D0%B

E%D0%BD%D0%B8_+%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA..PDF

3. Kalinichenko Z.D. Risk management: study guide / Dnipro: DDUVS, 2021. 224 p. URL: https://nemk.com.ua/wp-content/uploads/2024/04/%D0%9A%D0%B0%D0%BB%D1%96%D0%BD%D1%96%D1%87%D0%B5%D0%BD%D0%BA%D0%BE-%D0%97.-%D0%94.-%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA-%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82.-%D0%9D%D0%B0_%D0%B2%D1%87-%D0%BF%D0%BE%D1%81%D1%96%D0%B1.pdf

4. I. M. Posokhov, Managing risks in entrepreneurship: a study guide \ I. M. Posokhov. - Kharkiv: NTU "KhPI", 2015. - 220 c. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/722daaed-43f3-49f4-aa9b-beb5439cce13/content

5. Steshenko O. D. Riskology: Education. manual. - Kharkiv: UkrDUZT, 2019. - 180 p. URL: http://lib.kart.edu.ua/bitstream/123456789/2224/1/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf

6. Shklyaruk S. G. Management of financial risks: training. manual / S. G. Shklyaruk. — Kyiv: SE "Vyd. "Personal" house, 2019. — 494 p. URL: https://maup.com.ua/assets/files/lib/book/upr_fin_ryzik.pdf

7. Roeser Sabine Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk, Springer Science & Business Media, 2012, 1187 p. URL: https://books.google.com.ua/books/about/Handbook_of_Risk_Theory.html?id=PyJ_4KYwxNwC&redir_esc=y

Additional references

8. O. E. Arkhipov Information risks: research methods and methods, risk models and methods of their identification / O. E. Arkhipov, A. V. Skyba // Protection of information. – 2012. – Vol. 15. – No. 4. – P. 366–375. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/ITB-2015-s.12-16.pdf

9. Graivoronskyi M.V., Novikov O.M. "Security of information and communication systems"-K.: VHV Publishing Group.-2009.-608 c. URL: https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf

10. Danyk Y.G., Hryshchuk R.V. Fundamentals of cyber security: Monograph. - Zhytomyr: ZhNAEU, 2016. - 636 p.

11. Danyk Y.G. National security: prevention of critical situations:/ Yu.G. Danyk, Yu.I. Katkov, M.F. Pichugin - K.: Ministry of Defense of Ukraine, Zhytomyr: Ruta, 2006. - 388 p.

12. V. I. Dubrovin Decision-making in the process of project risk management / V. I. Dubrovin, V. M. Lyovkin. – Zaporizhzhia: ZNTU, 2012. – 196 p. URL: https://eir.zp.edu.ua/server/api/core/bitstreams/9ff5cbef-ce63-4108-b4bb-bcaa34e12651/content

13. Kaczynskii A.B. Security, threats and risk: scientific concepts and mathematical methods.-K.: IPNB, NA SBU.- 2004.-472 p. URL: https://scholar.google.com.ua/citations?view_op=list_works&hl=uk&hl=uk&user=-Jx2gWIAAAAJ

14. Kachynsky A.B. Safety of complex systems // A.B. Kaczynski. - K.: "Justion" LLC, 2017. - 494 p. URL: https://scholar.google.com.ua/citations?view_op=list_works&hl=uk&hl=uk&user=-Jx2gWIAAAAJ

15. Lysenko I. A. Methodical instructions for performing laboratory work in the academic discipline "Theory of Risks" [for students. full-time and part-time education. educational degree "Bachelor", specialty 125 Cybersecurity] Edition updated and supplemented / Comp. I. A. Lysenko – Kropyvnytskyi: National Technical University, 2018. – 32 p. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/a1b319d1-2373-4826-881a-48f18e0eaa89/content.

16. Technical risks. Theory and practice: [Electronic resource]: training. study guide / O.M. Terentiev, S. V. Zaichenko, A. Y. Kleschov, N. A. Shevchuk / KPI named after Igor Sikorsky. - Electronic test data (1 file: 5207 KB). Kyiv: KPI named after Igor Sikorskyi, 2020. – 168 p. URL: https://www.researchgate.net/profile/Anton-Kleshchov/publication/340022921_Tehnicni_riziki_Teoria_ta_praktikum/links/5e7325e34585152cdbfd7161/Tehnicni-riziki-Teoria-ta-praktikum.pdf

17. Danyk Y., Maliarchuk T., Briggs Ch. Hitting Home: Cyber-Hybrid Warfare in Ukraine and Its Impact on the United States the Georgetown Journal of International Affairs (GJIA), 02.2020, gjia.georgetown.edu. URL: https://www.researchgate.net/profile/Chad-Briggs/publication/320897341_Hybrid_War_High-

tech_Information_and_Cyber_Conflicts/links/60751d20299bf1f56d51d1a4/Hybrid-War-High-tech-Information-and-Cyber-Conflicts.pdf
18. Danyk Y., Maliarchuk T., Greg Simons Hybrid war and cyber-attacks: creating legal and operational dilemmas, Global Change, Peace & Security, ISSN: 1478-1158 (Print) 1478-1166 (Online) Journal homepage: https://www.tandfonline.com/loi/cpar20,https://doi.org/10.1080/14781158.2020.1732899
19. BS 7799-3:2006. Information security management systems. Guidelines for information security risk management. URL: https://ru.scribd.com/document/291784043/bs-7799-3-2006-open
20. ISO/IEC 16085:2006. Systems and software engineering – Life cycle processes – Risk management. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=71810
21. NIST Special Publication 800-30 – Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards. URL: https://www.archives.gov/files/era/recompete/sp800-30.pdf
22. Information Security Management. Part 2. Specification for Information Security Management systems. British Standard BS 7799, Part 2. 2000. URL: http://www.asq0511.org/Presentations/200405/BS7799_Implementation_ASQ_12May04.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;
- credit test: 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	Date, signature 28.08.2024	Head of the department Serhii YEVSEIEV
	Date, signature 28.08.2024	Guarantor of the educational program Serhii YEVSEIEV