Syllabus
Course Program

Organising document management with restricted access

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
8

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 "Organization of document circulation with limited access" is a normative educational discipline. The discipline is aimed at the student's acquisition of theoretical knowledge and practical skills regarding the organization of document circulation with limited access in the field of cyber protection.

Course objectives and goals

Mastering by students a set of knowledge in the field of record keeping, storage, use and destruction of documents and other material carriers of information containing official information with limited access.

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 - 24 hours, laboratory classes - 12 hours, self-study - 54 hours.

Course prerequisites

Information security of the state, Cyber security. Legal aspects and technologies, Physical foundations of technical means of intelligence.

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 theoretical principles of legal regulation of information with limited access.
Concept of information and its features. Restricted information in doctrine and law. General characteristics of types of information with limited access.
Topic 2. Concept and legal content of personal data as an object of legal protection in Ukraine.
The concept of personal data as an object of legal protection and their place in legal relations. General requirements for processing personal data in databases. State control in the field of personal data circulation.
Topic 3. Modern trends in the use of information with limited access in institutions.
Threats from unauthorized leakage of information with limited access. Peculiarities of staffing of information protection units with limited access in institutions. Use of monitoring measures in the field of information protection with limited access.
Topic 4. Peculiarities of handling information with limited access in the process of business activity.
Concepts, signs, principles and types of entrepreneurial activity. Concept, meaning, threats and components of business security. Protection of information with limited access at the enterprise.
Topic 5. Basics of technical protection of information in modern information systems.
Classes of tasks for technical protection of information in information systems. Protection of information from leakage through technical channels. Protection of information from unauthorized access.
Topic 6. Protection of electronic information.
Means and methods of detecting and blocking technical channels of acoustic information leakage. Protection of acoustic information from being intercepted by radio jamming devices. Methods of searching for radio-trading devices. Protection of information from leakage through technical channels formed by auxiliary technical means. Protection of information from unauthorized recording by sound recording devices. Protection of written information from optical removal.
Topic 7. Maintenance of documents containing confidential information marked "For official use".
Acceptance, review and registration of documents. Reproduction and distribution of documents. Formation of executed documents. Use of documents. Destruction of documents.
Topic 8. Organization of work with secret documents.
Classification and registration of documents. Equipment of premises for storage of material carriers of secret information. Acceptance and processing of correspondence. Printing materials.
Registration and sending of documents. Preliminary and inventory accounting of documents.
Topic 9. Legal responsibility in the field of information circulation with limited access.
Theoretical principles of legal responsibility in the field of information circulation with limited access. Characteristics of offenses in the field of information circulation with limited access. Criminal offenses in the circulation of information with limited access. Administrative offenses in the sphere of circulation of information with limited access. Civil offenses in the circulation of information with limited access. Disciplinary offenses in the circulation of information with limited access.
Topic 10. Document and documentation support of management in Ukraine.
The system of state bodies, state enterprises and state institutions of Ukraine. Systems of state bodies of Ukraine. Legislative regulation of record keeping and documentation in state institutions of Ukraine. Standardization, unification and stenciling of management documents. Documenting management information in state institutions. Forms of organizational and administrative documents. Seals of state institutions. Dating and approval of management documents. Approval and signing of management documents. General requirements for the text of administrative documents. Peculiarities of preparation and registration of executive documents. Certification of copies and extracts of official documents. Registration of documents. Organization of the transfer of documents and their execution and control over the execution of documents.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Organizational work on the protection of information with limited access in NATO and EU countries.
Topic 2. Study of the international standard for assessing the security of information technologies (ISO/IEC 15408).
Topic 3. Study of the organizational work of the information protection service in automated systems.

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. Rybalskyi O.V., Khakhanovskyi V.G., Kudinov V.A. Basics of information security and technical protection of information. Guide for cadets of the Ministry of Internal Affairs of Ukraine. - K.: Ed. of the National Academy of Internal Affairs. cases, 2012. – 104 p.
https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf
2. Organization of protection of information with limited access: training. guide/A.M. Huz, I.P. Kasperskyi, S.O. Knyazev and others. - K. Nats. Acad., SBU, 2018. – 252 p.
http://za.inf.ua/bo/oziod18.pdf
3. Organizational work on information protection in information and communication systems (workshop). Educational and methodological manual for independent work of a student from a course of choice// Shuaibov O. K. - Uzhgorod, State Higher Secondary School "UzhNU", "Hoverla". 2011. – 98 p.
https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/20031/1/MET-ORG-ROB- ZACH-INF-11.pdf
4. A practical guide for organizing electronic document flow and controlling access to confidential data. "Document and Records Management" – Waddington, P.
https://www.osa.tas.gov.au/wp-content/uploads/2023/08/Advice-54-Records-Management-Toolkit-for-LG-Fact-Sheet-1-Mail-Processing.pdf
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.

Additional literature:

6. On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI. Update date: 10/27/2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
7. On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII. Date of update: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
8. DSTU 3396 0-96 Information protection. Technical protection of information. Basic provisions. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf.
9. 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

10. DSTU ISO/IEC 15408-1:2023 Information technologies. Protection methods. Evaluation criteria. Part 1. Introduction and general model (ISO/IEC 15408-1:2022, IDT).
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104382
11. DSTU ISO/IEC 15408-2:2023 Information technologies. Cyber security and privacy protection. IT security evaluation criteria. Part 2. Safety functional components (ISO/IEC 15408-2:2022, IDT).
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104383
12. DSTU ISO/IEC 15408-3:2023 Information technologies. Cyber security and privacy protection. IT security evaluation criteria. Part 3. (ISO/IEC 15408-3:2022, IDT).
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104388
13. On the approval of the Standard Instruction on the procedure for record-keeping, storage, use and destruction of documents and other material carriers of information containing official information: Resolution of the Cabinet of Ministers of Ukraine dated October 19, 2016 No. 736. Date of update: 08/25/2023. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text.

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