Syllabus

Course Program

Legal regulation of 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 Special (professional), Mandatory
Semester 2	Language of instruction English

Lecturers and course developers

Vladyslav KHVOSTENKO

vladyslav.khvostenko@khpi.edu.ua

Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

The author of more than 30 publications: of them 3 monographs in co-authorship and 1 handbook with a neck. Leading lecturer in the disciplines: "Intellectual property of security systems", "Legal regulation of cyber security", "Strategic communications in conditions of hybrid warfare", "Fundamentals of systems theory and system analysis".
More about the lecturer on the department's website

General information

Summary

The educational discipline "Legal regulation of cybersecurity" is a mandatory educational discipline. The study of the discipline is aimed at the skills and competencies to determine the place and role of cyber security in the overall system of national security, legal regulation of the state and principles of ensuring cyber security of the individual, society and the state, necessary for further work and to teach them to apply methods and means of effective and safe handling of information independently from its origin and type in conditions of widespread use of modern information technologies.

Course objectives and goals

Formation of students' theoretical knowledge on the basics of strengthening the quality of security sector management with the help of effective and efficient security provision in conditions of democratic supervision and control.

Format of classes

Lectures, workshops, consultations, self-study. Final control - credit test.

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
GC-8. Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.

Learning outcomes

LO-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LO-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LO-3. Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity.
LO-4. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.
LO-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LO-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LO-7. Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cyber security.
LO-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LO-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LO-10. Perform analysis and decomposition of information and telecommunication systems.
LO-11. Perform analysis of connections between information processes on remote computer systems.
LO-12. Develop threat and intruder models.
LO-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by hardware and software tools and evaluate the effectiveness of the quality of the decisions made.
LO-15. Use modern hardware and software of information and communication technologies.
LO-16. Implement complex information security systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. Ensure the processes of security and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of security of electronic information resources with a reflection of relationships and information flows, processes for internal and remote components.
LO-18. Use software and software-hardware complexes for the security of information resources.
LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.

LO-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LO-21. Solve tasks of provision and support (including: review, testing, accountability) of the access control system according to the stated security policy in information and telecommunication (automated) systems.
LO-22. Solve the management procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and/or cyber security.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LO-24. Solve the problems of managing access to information resources and processes in information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based).
LO-25. Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and telecommunication (automated) systems using event registration logs, their analysis and stated protection procedures.
LO-26. Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems.
LO-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.
LO-29. Evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means under the conditions of realization of threats of various classes.
LO-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.
LO-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LO-32. Solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the stated security policy.
LO-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LO-34. Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization.
LO-35. Solve the tasks of providing and supporting complex information security systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the stated policy of information and/or cyber security.
LO-36. Detect dangerous signals of technical means.
LO-37. Measure the parameters of dangerous and interfering signals during the instrumental control of information security processes and determine the effectiveness of information security against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system.
LO-38. Interpret the results of special measurements using technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information security system.
LO-39. Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents.
LO–40. Interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information security system.
LO-41. Ensure the continuity of the event and incident logging process based on automated procedures.

LO-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LO-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LO-44. Solve the problems of ensuring the continuity of the organization's business processes on the basis of risk management theory and the stated information security management system, in accordance with national and international requirements and standards.
LO-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LO-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LO-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
LO-48. Implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.
LO-49. Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.
LO-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LO-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LO-52. Use tools for monitoring processes in information and telecommunication systems.
LO-53. Solve problems of software code analysis for the presence of possible threats.
LO-54. Be aware of the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 32 hours, workshops - 16 hours, self-study - 72 hours.

Course prerequisites

Introduction to the specialty. Introductory practice, Information security of the state.

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. Concept, subject, method and place in the information law system of Ukraine.
The concept of information law as a field of law. Conceptual approaches to the formation of the content of information law. Subject and methods of information law. Principles of information law.
Sources of information law.
Topic 2. Information society: concepts, basic principles of development in Ukraine, relationship with information culture and information security.
Information society and information civilization: concepts, positive and negative aspects. Concept and essence of informatization. Basic principles of information society development in Ukraine. Information policy at the current stage. Information security: concepts, types. Concept of information culture.
Topic 3. Informational legal relations: concept, content, types.
The concept of informational legal relations and their content. Subject and objects of informational legal relations. Concepts, legal signs and types of information. Legal status of information as an object of civil

rights. Information as an object of ownership. The content of the subjective right to information. Subjects of informational legal relations. Classification of informational legal relations.

Topic 4. Information activity: concepts, types.

The concept of information activity. Main directions and types of information activities. Information activity of state authorities. Coverage of the activities of state authorities and local self-government bodies in Ukraine.

Topic 5. Legal regulation of print mass media, information agencies, publishing, library and archival business and state statistics in Ukraine.

Print mass media (press) in Ukraine: legal status, state registration, editorial and publishing activity, state support and social protection of journalists. Information agencies: concepts, features of creation and registration, creation and distribution of their products Library activity in Ukraine: general principles, library system, rights and responsibilities of readers. Archival activity in Ukraine: National archival fund and system of archival institutions. Publishing business in Ukraine: organization, subjects, state registration. Book Chamber of Ukraine. Legal regulation of state statistics in Ukraine.

Topic 6. Legal regime of information with limited access.

Concepts and types of information with limited access about a person. Protection of personal data. Protection of confidential information that is the property of the state (official information). State secret in Ukraine.

Topic 7. Liability for offenses in the field of information relations.

Concepts and types of offenses in the information sphere. Civil offenses in the information sphere. Disciplinary responsibility in the field of informational legal relations. Administrative responsibility for offenses in the information sphere. Criminal liability for crimes in the information sphere. Information law sanctions contained in separate acts of the legislation of Ukraine.

Topics of the workshops

Topic 1. Concept, subject, method and place in the information law system of Ukraine.
Topic 2. Information society: concepts, basic principles of development in Ukraine, relationship with information culture and information security.
Topic 3. Informational legal relations: concept, content, types.
Topic 4. Information activity: concepts, types.
Topic 5. Legal regulation of print mass media, information agencies, publishing, library and archival affairs and state statistics in Ukraine.
Topic 6. Legal regime of information with limited access.
Topic 7. Liability for offenses in the field of information relations.

Topics of the laboratory classes

Not provided for in the curriculum.

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:
Discovering Entrepreneurship, Engaging Stakeholders for Success
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. About the media: Law of Ukraine edition dated 01.01.2024 No. 2849-IX // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/2849-20#n2349
2. On state secrets: the Law of Ukraine, edition of 01.01.2024 No. 3855-XII // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/3855-12#Text
3. About banks and banking activity: Law of Ukraine, edition dated 01.01.2024 No. 2121-III // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/2121-14#Text
4. On the protection of personal data: Law of Ukraine edition dated 10.27.2022 No. 2297–VI // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. On operational and investigative activity: Law of Ukraine, edition of 31.03.2023 No. 2135-XII // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/2135-12#Text
6. Civil Code of Ukraine: Law of Ukraine edition of 30.01.2024 No. 435-IV // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/435-15#Text
7. On cloud services: Law of Ukraine, edition of 12.27.2023 No. 2075-IX // VVR of Ukraine. https://zakon.rada.gov.ua/laws/main/2075-20#Text
8. On state support of the media, guarantees of professional activity and social protection of journalists: Law of Ukraine edition dated 03.31.2021 No. 540/97-BP // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text
9. About libraries and library affairs: Law of Ukraine, edition of 01.01.2022 No. 32/95-BP // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/32/95-%D0%B2%D1%80#Text
10. On the publishing business: Law of Ukraine, edition dated 12.31.2023 No. 318/97-BP // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/318/97-%D0%B2%D1%80#Text
11. On the mandatory copy of documents: Law of Ukraine, edition of 31.03.2023 No. 22-23, Article 199 // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/595-14#Text
12. On the national archival fund and archival institutions: Law of Ukraine edition dated 07.02.2023 No. 3814-XII // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/3814-12#Text
13. On scientific and scientific-technical activity: Laws of Ukraine edition dated 04.01.2024 No. 848-VIII // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/848-19#Text
14. On access to public information: Laws of Ukraine edition dated 08.10.2023 No. 2939-VI // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/2939-17#Text
15. On the appeal of citizens: Laws of Ukraine edition dated 12.31.2023 No. 393/96-BP // VVR of Ukraine. https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text.

Additional literature:

16. Yevseyev S.P. Cyber security: modern protection technologies. / Evseev S.P., Ostapov S.E., Korol O.G. // Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678. - Access mode: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
17. Information security. Textbook / V. V. Ostroukhov, M. M. Prysiazhnyuk, O. I. Farmagey, M. M. Chekhovska, etc.; under the editorship V. V. Ostroukhova - K.: Lira-K Publishing House, 2021. - 412 p. https://lira-k.com.ua/preview/12867.pdf
18. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. https://drive.google.com/drive/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
19. 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/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
20. 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/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Assessment and grading

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

Points are awarded according to the following ratio:

- workshops: 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	28.08.2024	Head of the department Serhii YEVSEIEV
	28.08.2024	Guarantor of the educational program Serhii YEVSEIEV