Syllabus
Course Program

Intrusion detection

Specialty
113 Applied mathematics

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Intelligent Data Analysis

Department
Cybersecurity

Level of education
Bachelor's level

Course type
Special (professional), Selective

Semester
8

Language of instruction
Ukrainian

Lecturers and course developers

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 discipline “Detection of Secondaries” is an elective discipline. The discipline is aimed at identifying information that needs to be protected at critical infrastructure facilities (CIF). Mastering the methods and means of technical protection of information at critical infrastructure facilities. Familiarization with the channels of information leakage and the reasons for their formation. Mastering the skills of working with tools and complexes for detecting embedded devices for unauthorized information acquisition. Mastering the skills of working with the means and complexes of information protection at the CI. Mastering the procedure for inspecting and analyzing CII to ensure information security. Mastery of organizational and technical measures to protect information at the CIP.

Course objectives and goals

Teaching students the principles of determining the general requirements for cybersecurity of critical infrastructure facilities, establishing a list of basic cybersecurity measures to be implemented at a critical infrastructure facility based on the requirements of international information security standards, state

regulations on information security technology, determining the procedure and criteria for classifying facilities as critical infrastructure facilities.

Format of classes

Lectures, laboratory classes, calculation tasks, consultations. Final control – exam.

Competencies

GC 1. Ability to learn and master modern knowledge.
GC 2. Ability to apply knowledge in practical situations.
GC 4. Ability to be critical and self-critical.
GC 6. Ability to abstract thinking, analysis and synthesis.
GC 8. Knowledge and understanding of the subject area and understanding of professional activities.
SC 3. Ability to choose and apply mathematical methods for solving applied problems, modeling, analysis, design, management, forecasting, decision-making.
SC 5. Ability to develop algorithms and data structures, software tools and program documentation.
SC 7. Ability to solve professional problems with the help of computer equipment, computer networks and the Internet, in the environment of modern operating systems, using standard office applications.
SC 8. Ability to operate and maintain software of automated and information systems for various purposes.
SC 10. Ability to conduct mathematical and computer modeling, data analysis and processing, computational experiment, solving formalized problems using specialized software.

Learning outcomes

LO 2. Master the basic principles and methods of mathematical, complex and functional analysis, linear algebra and number theory, analytical geometry, theory of differential equations, including partial differential equations, probability theory, mathematical statistics and random processes, numerical methods.
LO 24. Be able to apply existing and develop new algorithms and software tools for processing measurement and observation data, texts, signals and images.
LO 25. be able to apply modern information technologies and software for processing large amounts of data based on distributed and cloud services.

Student workload

The total volume of the course is 150 hours (5 ECTS credits): lectures - 20 hours, laboratory classes - 30 hours, self-study - 100 hours.

Course prerequisites

“Mathematical Analysis, Linear Algebra, Analytical Geometry, Fundamentals of Cryptology, Databases and Information Systems.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1: General requirements for cybersecurity of critical infrastructure.
List of basic requirements for ensuring cybersecurity of critical infrastructure.
Topic 2. Physical protection of critical infrastructure facilities.

Stories of battles. Hackers. The impact of threats. Modern security monitoring and control center (SOC). Protection of infrastructure communications.

Topic 3. Cyber defense of infrastructure.

The main cyber threats to critical infrastructure. Attackers and their tools.

Topic 4. Crisis management and consequence management.

How to organize effective crisis management in critical infrastructure. Implementation of the concept on the example of the OSC of Ukraine. Threat classifier. Improved model of the ABS infrastructure. Conceptual and synergistic security models. Improvement of the security assessment model. Coordination of actions of different agents during a crisis situation.

Topic 5. Protection of telecommunication infrastructure.

How to protect telecommunication networks from cyber attacks. Segmentation and micro-segmentation of the network. Monitoring and centralized management. Next Generation Firewall (NGFW). Unified threat management (UTM). Inspection of encrypted traffic. Protection against the leakage of confidential information. Implementation of two-factor authentication solutions. Combining local networks and remote access.

Topic 6 Protection of the electric power infrastructure.

Threats and vulnerabilities to the electric power infrastructure. Attacks on the Internet of Things infrastructure. Strategies and technologies for protecting electricity infrastructure. Challenges facing international cooperation in the field of energy infrastructure protection.

Topic 7. Protection of financial infrastructure.

The main threats and risks to financial infrastructure, tools for their identification and assessment. Methods and technologies for protecting financial transactions and data in banks and financial institutions. Standards and regulatory requirements to ensure the security of financial infrastructure. Current trends and innovations in cybersecurity to protect financial systems and infrastructure.

Topic 8: International cooperation in the protection of critical infrastructure.

International organizations and initiatives to coordinate critical infrastructure protection measures between countries. International treaties and mechanisms of cooperation to ensure the security of critical infrastructure. Green Paper on Critical Infrastructure Protection in Ukraine. Sectors, facilities, systems that can be classified as critical infrastructure. Main threats to critical infrastructure. State policy of critical infrastructure protection. Strategic goals of the state policy of critical infrastructure protection. Basic principles of critical infrastructure protection in Ukraine. The system of critical infrastructure protection in Ukraine. Development of mechanisms for the protection of critical infrastructure in Ukraine.

Topic 9. Conditions for the emergence of a terrorist threat and countermeasures.

Analysis of the essence and content of the problem of information security of the state at the present stage of development of science and technology. Factors of the origin of terrorism. Options for classifying terrorism. Types of terrorists. Motives of terrorists. Methods of increasing the level of cyber defense of critical information structure.

Topic 10. Tools for managing information security risks of critical infrastructure.

Information security risk management tools / Digital Securit risk assessment models. Model of threat and vulnerability analysis. The principle of the algorithm. Calculation of risks by information security threat. Tasks of countermeasures. Payment infrastructure.

Topic 11. Management system as an object of cybersecurity.

Analysis of the control system as an object of cybersecurity. Features of the analysis. Basics of detection and search of objects with critical cyber infrastructure

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1: Study of general requirements for cyber defense of critical infrastructure.

Topic 2. Critical infrastructure by regions of Ukraine. Organizational principles of the region of Ukraine as components of the national system of critical infrastructure protection.

Topic 3. Compilation of information about the critical information infrastructure facility of a particular region of Ukraine.

Topic 4. Study of the features of the national critical infrastructure protection system.

Topic 5. Study of the peculiarities of the formation of Technical Requirements for the creation of specialized software "State Register of Critical Information Infrastructure Objects".
Topic 6. Study of measures to ensure cyber security of critical information infrastructure of banks.
Topic 7. Methodological recommendations for the development of current and target cybersecurity profile. Methodological recommendations for analyzing the current and target cybersecurity profile.
Topic 8: Classification of cybersecurity measures for critical infrastructure facilities.

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. The Law of Ukraine "On Critical Infrastructure", dated November 16, 2021, No. 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. The Cabinet of Ministers of Ukraine "On Approval of the General Requirements for the Cyber Defense of Critical Infrastructure Objects", June 19, 2019, No. 518. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
3. Resolution of the Cabinet of Ministers of Ukraine "Some Issues of Critical Information Infrastructure Objects", October 9, 2020, No. 943. https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
4. Methodological recommendations for improving the level of cyber defense of critical information infrastructure. Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine of October 06, 2021, No. 601. https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
5. Law of Ukraine "On Critical Infrastructure". https://zakon.rada.gov.ua/laws/show/1882-20#Text
6. Resolution of the Board of the National Bank of Ukraine "On Approval of the Regulation on the Organization of Cyber Defense in the Banking System of Ukraine". https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
7. Cybersecurity: modern protection technologies. Textbook for students of higher educational institutions. / S.E. Ostapov, S.P. Yevseev, O.G. Korol. - Lviv: Novyi Svit-2000, 2020. - 678 p. https://profbook.com.ua/index.php?route=product/product/download&product_id=2663&download_id=1094.
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others: PC TECHNOLOGY CENTER, 2021. - 188 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others: PC TECHNOLOGY CENTER, 2023. - 168 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others: PC TECHNOLOGY CENTER, 2022. - 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Additional references

11. ISO/IEC 27001:2022- [Accessed at: https://www.iso.org/ru/standard/27001
12. ISO/IEC 27002:2022- [Accessed at: https://www.iso.org/standard/75652.html].
13. ISO/IEC 27005:2022- [Accessed at: https://www.iso.org/standard/80585.html].

Assessment and grading

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

Points are awarded according to the following ratio:
- laboratory work: 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	Date, signature		
	29.08.2024		Head of the department Serhii YEVSEIEV
	Date, signature 29.08.2024		Guarantor of the educational program Olena AKHIIEZER