Syllabus
Course Program

Information security management

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
5

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 161, including 18 utility model patents, 11 monographs, of which 6 collective monographs, 18 training manuals, 66 articles in foreign publications and specialized publications of Ukraine, including in the Scopus scientometric database. Leading lecturer in the disciplines: "Fundamentals of social engineering", "Information security of the state", "Information security management", "Organization of document circulation with limited access", "Security in social networks".

More about the lecturer on the department's website

General information

Summary

The educational discipline "Information security management" is an optional educational discipline. The discipline is aimed at the student's acquisition of theoretical knowledge and practical skills in information security management in information and telecommunication (automated) systems for the implementation of the established security policy.

Course objectives and goals

Formation of students' theoretical knowledge of the basic management principles of incident and risk management based on the requirements of international regulators.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control in the form of an credit test.

Competencies

GC 2. Ability to apply knowledge in practical situations.
GC 3. The ability to generate new ideas (creativity).
GC 6. Ability to abstract thinking, analysis and synthesis.
GC 7. Ability to search, process and analyze information from various sources.
GC 9. Ability to communicate with representatives of other professional groups of various levels (with experts from other fields of knowledge/types of economic activity)
GC 10. Skills in the use of information and communication technologies.
GC 13. Skills of interpersonal interaction.
SC 7. The ability to solve professional tasks using 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 9. Ability to use modern technologies of programming and software testing.
SC 14. The ability to understand the statement of the task, formulated in the language of a certain subject area, to search and collect the necessary initial data.

Learning outcomes

LO 7. To be able to conduct practical research and find a solution to incorrect problems.
LO 11. To be able to apply modern technologies of programming and software development, software implementation of numerical and symbolic algorithms.
LO 18. Effectively communicate information, ideas, problems and solutions with specialists and society in general.
LO 19. Collect and interpret relevant data and analyze complexities within the scope of one's specialization to make judgments that reflect relevant social and ethical issues.
LO 24. To be able to apply existing and develop new algorithms and software tools for processing measurement and observation data, texts, signals and images.
LO 25. To be able to apply modern information technologies and software for processing large data sets based on distributed and cloud services.

Student workload

The total volume of the course is 90 hours (3 ECTS credits): lectures - 28 hours, practical classes - 16 hours, self-study - 46 hours.

Course prerequisites

"Algorithmization and programming", "Discrete structures and data structures".

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 concept of information security of the state and components of national interests of Ukraine in the information sphere.
Basic terms and concepts of IS. Evolution of cyber threats. Critically important infrastructures of the states of Ukraine and the USA. Cyber operation "Olympic Games". Cyber attack on the Rivne NPP. A billion dollar carbanaki cyber attack. CISCO's report on information security for the first half of 2017. Analysis of methods of deployment of malicious software. History of incidents - 2008, speculation?. History of incidents - 2012. Are the risks real? Threats today. The current situation in the security of ACSTP. Vulnerabilities: the human factor. Cybersecurity issues in the Internet of Things. The main causes of cyber

violations. Relevance of incident management. Basic concepts of incident management. Incident management requirements according to the ISO/IEC 27001 standard. Incident management process model according to the ISO/IEC 27035 standard. Signs of IS incidents. Objectives of incident management. Standards, recommendations and best practices in the field of incident management.

Topic 2. Information security incident management.

A brief overview of the problem of risk management. Integration of risk management in the life cycle of system development (system development life cycle, sdlc). ISO/IEC 27001 standard. Life cycle of IT systems. Risk assessment methodology. Characteristics of systems. Identification of threats. Vulnerability identification. Analysis of control (management). Definition of opportunity (opportunity). Analysis of impact (impact). Definition of risk. Recommendations for control (management). Documentation of results. Risk reduction. General consistency of actions in risk reduction methodology. Profitability analysis and residual risk. Key factors of successful risk management.

Topic 3. Peculiarities of incident management according to the requirements of the ITIL international standard.

The construction concept, structure and functional features of an effective IS incident management system. Peculiarities of incident management according to the requirements of the ITIL international standard.

Topic 4. The concept of a cyber incident response team (CERT / CSIRT): history of development and possible benefits of adoption.

Generalized classification of CERT / CSIRT groups: scope, objectives and potential clients. The concept of a cyber incident response team (CERT / CSIRT): development history and possible benefits to the enterprise.

Topic 5. Toolkit for the effective functioning of IS response teams.

Documentation support of the IS incident management process. Activities of various IS response groups. A toolkit for the effective functioning of IS response teams.

Topic 6. Documentation of the IT incident management process.

Examples of documents: private (corporate) policy of IIB management. Activities of IS response teams (USA) . Why companies need a SOC. How to implement SOC in the organization. Gather a team of experts. Stay up to date with new threats. Provide the infrastructure to support the SOC. SOC models in the NIST CYBERSECURITY FRAMEWORK notation. Tools and data quality. Detection. Abstract network security tools. The cost of incorrect work. Amount of data. A sample list of questions during software and technical examination of IS after the action of incidents. Sample lists after being affected by IS incidents.

Topic 7. Analysis of risks in the field of information protection.

Evolution of threats. CISCO recommendations.

Topic 8. Risk management and international standards.

International standard iso 31000. Stages of the risk management process. Ukrainian State Center of Radio Frequencies. Framework program on cyber security. The basis of the framework program. The main functions of the framework program. Levels of implementation of the framework program. Framework program on cyber security. Establishing or improving a cybersecurity program.

Topic 9. Risk analysis technologies.

Information security audit. Examination of the ITS computing system. Examination of the IT information environment. Examination of the physical environment of IT. Survey of the user environment. ITS vulnerability testing. Bank information security audit. Risk assessment methods. Practical risk management. CRAMM methodology. RiskWatch methodology. Methodology Microsoft.

Topic 10. Information security policies.

Policy structure. IS policy (example). Identification and valuation of assets. Analysis of sources of problems. IS roles and responsibilities. Distribution of duties. Contacts with authorized bodies. Contacts with groups of specialists on certain issues. An example of security work in agreements with third parties. IS in project management. Mobile equipment and remote work. Remote work. Personnel safety. Terms and conditions of employment. Management responsibility. IS awareness, education and training. Termination or change of terms of employment. Asset management. Ownership of SMIB assets.

Topic 11. Information security management system policy.

Information security management system. Approximate sequence of actions in the development of SMIB. Mandatory documents of SMIB. The general information security policy may include the following information. An example of the structure (general and detailed) of the organization's security policies (to ensure network security). An example of an information security policy. Examples of failed policies. Other signs of bad documents. Factors determining the effectiveness of the security policy. Content of standard

27001:2013. The context of the organization. leadership Planning. Information security risk assessment. Information security risk management. Statement of applicability (statement of applicability). Target indicators in the field of information security and planning for their achievement. Software. Documented information. What should be documented? Management of documented information. Functioning. Assessment of activity results. Improvement.

Topic 12. Security audit and risk analysis.

Relationship of concepts. Qualitative evaluation of SMIB. Content of the incident management process. Causes of incidents. Specific information security incident management issues are addressed in the following documents. Planning and preparation. Incident Investigation Team. The structure of the incident investigation team. Development of regulatory documents on incident management. The principles of an effective policy of response to incidents ib. Information security incident investigation policy. Information security incident investigation resources and tools. Preventive measures. Identification and analysis of information security incidents. Signs of an information security incident. Analysis of information security incidents. Information security incident documentation. Sending information security incident notifications. Countering the spread of the incident. The procedure for eliminating the consequences of an IS incident.

Topic 13. Protection and analysis of end devices.

Protection against malicious programs. Host-level intrusion protection. Application security. Network and server profiling. General vulnerability assessment system. Common Vulnerability Assessment System (CVSS). Compliance architectures. Secure device management. Information security management systems.

Topic 14. Security monitoring.

Monitoring of the most common protocols. Security technologies. Types of security data. Session and transaction data. End device logs. Network magazines.

Topic 15. Analysis of intrusion data.

Sources of warnings. Alert Score Overview. A common data platform. Network data research. Increasing the effectiveness of cyber security analysts. Evidence processing and attribution of attacks.

Topic 16. Response to incidents and their processing.

Incident response models. Incident handling.

Topics of the workshops

Topic 1. Deployment of the operating system for auditing information security of computer networks and systems.
Topic 2. Tools for covert collection of technical information from a computer system or network.
Topic 3. Investigation of vulnerabilities of systems and web resources using specialized vulnerability scanners (Nessus, Vega).
Topic 4. Determination of vulnerabilities of web resources and web applications. Vulnerability scanner – Vega.
Topic 5. Searching for vulnerabilities and sensitive information in open resources using Maltego.
Topic 6. Collection of technical and sensory information using class software - sniffers.
Topic 7. Aircrack-ng, a means of researching the vulnerabilities of wireless Wi-Fi networks.
Topic 8. Snort rules and firewall rules.
Topic 9. Extracting an executable file from PCA.
Topic 10. Interpretation of HTTP and DNS data to isolate an attacker.
Topic 11. Incident handling.

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, prepare for laboratory work, control work and credit test.

Course materials and recommended reading

References

1. Management of information security: study guide for students of specialty 125 "Cyber security" / O.G. Korchenko, M.E. Shelest, S.V. Kazmirchuk, Yu.M. Tkach, E.V. Ivanchenko. – Nizhin: FOP Lukyanenko V.V. TPK "Orkhideya", 2019. - 408 p. : fig.
http://ir.stu.cn.ua/bitstream/handle/123456789/19244/%d0%9c%d0%b5%d0%bd%d0%b5%d0%b4%d0%b6%d0%bc%d0%b5%d0%bd%d1%82%20%d1%96%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0% b7%d0%bf.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
2. 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
3. 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
4. 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

Additional references

5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems.
https://www.iso.org/ru/standard/27001
6. Methodological recommendations for the implementation of the information security management system and risk assessment methods in accordance with the standards of the National Bank of Ukraine/ [Electronic resource].
https://zakon.rada.gov.ua/laws/show/v0365500-11#Text
7. DSTU ISO/IEC TR 13335-1:2003 Information technologies. Information technology security management guidelines. Part 1. Concepts and models of information technology security. [Electronic resource].
http://lindex.net.ua/ua/shop/bibl/500/doc/11423
8. DSTU ISO/IEC TR 13335-2:2003 Information technologies. Part 2. Information technology security management guidelines. [Electronic resource].
http://www.premier-hs.com.ua/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsinikh-tiekhnologhii Date of application: December. 7.2017.
9. DSTU ISO/IEC TR 13335-3:2003 Information technologies. Information technology security management guidelines. Part 3. Methods of managing the protection of information technologies. [Electronic resource].
http://lindex.net.ua/ua/shop/bibl/500/doc/11425
10. DSTU ISO/IEC TR 13335-4:2005 Information technologies. Information technology security management guidelines. Part 4. Selection of means of protection. [Electronic resource].
http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005
11. DSTU ISO/IEC TR 13335-5:2005 Information technologies. Information technology security management guidelines. Part 5. Guidelines for Network Security Management. [Electronic resource].
http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

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
29.08.2024

Head of the department
Serhii YEVSEIEV

Date, signature
29.08.2024

Guarantor of the educational program
Olena AKHIIEZER