Syllabus
Course Program

Fundamentals of cybersecurity

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
6

Language of instruction
Ukrainian

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 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

General information

Summary

The educational discipline "Basics of cyber security" is an optional educational discipline. The study of the discipline is aimed at mastering the necessary basic concepts and rules of safe behavior on the network, familiarizing students with the principles of building information protection systems, familiarizing them with the main mechanisms of security services, studying information security management, teaching students the basics of information security audits, as well as students studying special mechanisms of cyber protection.

Course objectives and goals

Teaching students the principles of building information protection systems, researching and using modern procedures for ensuring the provision of basic information security services in cyberspace, conducting an audit of the current state of information security.

Format of classes

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

Competencies

GC 1. The ability to learn and master modern knowledge.
GC 6. Ability to abstract thinking, analysis and synthesis.
GC 8. Knowledge and understanding of the subject area and understanding of professional activity.
GC 12. Determination and persistence in relation to assigned tasks and assumed responsibilities.
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 of various purposes.
SC 9. The ability to use modern technologies of programming and testing of software

Learning outcomes

LO 11. To be able to apply modern technologies of programming and software development, software implementation of numerical and symbolic algorithms.
LO 16. Demonstrate the skills of interaction with other people, the ability to work in a team.
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

"Mathematical analysis", "Linear algebra", "Analytic geometry", "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

Cisco Networking Academy:
Topic 1. Cyber security - the world of specialists and criminals.
The world of cyber security. Cybercriminals versus cyber security professionals. General threats. The spread of cyber security threats. Training of more specialists.
Cisco Networking Academy:
Topic 2. Cube of cyber security.
Triad of the Central Committee (CIA). Data states. Cyber security countermeasures. Structure of IT security management.

Cisco Networking Academy:
Topic 3. Cyber security - threats, vulnerabilities and attacks.
Malware and malicious code. Fraud. Attacks
Cisco Networking Academy:
Topic 4. The art of protecting secrets.
Cryptography. Access control. Data hiding.
Cisco Networking Academy:
Topic 5. The art of ensuring data integrity.
Types of data integrity controls. Digital signatures. Certificates. Ensuring the integrity of databases.
Cisco Networking Academy:
Topic 6. The concept of five nines.
High availability. Measures to improve accessibility. Reaction to the incident. Emergency recovery.
Cisco Networking Academy:
Topic 7. Protection of the cyber security domain.
Protection of systems and devices. Strengthening the protection of servers. Strengthening network protection. Physical security.
Cisco Networking Academy:
Topic 8. How to become a cyber security specialist.
Domains of cyber security. Understanding work ethics in cyber security. The next step.

Topics of the workshops

Cisco Networking Academy:
Topic 1. Authentication, authorization and accounting.
Cisco Networking Academy:
Topic 2. Install a virtual machine on a personal computer.
Cisco Networking Academy:
Topic 3. Detection of threats and vulnerabilities.
Cisco Networking Academy:
Topic 4. Use of steganography.
Cisco Networking Academy:
Topic 5. Hacking passwords.
Cisco Networking Academy:
Topic 6. Use of digital signatures.
Cisco Networking Academy:
Topic 7. Remote access.
Cisco Networking Academy:
Topic 8. Protection of Linux systems.

Topics of the laboratory classes

This field is filled in the same way if the curriculum laboratory classes.

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:
PaloAlto (Cybersecurity Foundation)

https://paloaltonetworksacademy.net/course/index.php.

Course materials and recommended reading

Basic literature:

1. Yevseyev S.P. Cyber security: modern protection technologies. / Yevseev S. P., Ostapov S. E., Korol O. G. // Study guide for students of higher educational institutions. Lviv: "New World - 2000", 2019. - 678. http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Cybersecurity in the modern world: materials of the 3rd All-Ukrainian scientific and practical conference (Odesa, November 19, 2021) / edited by O. V. Dyky; editor: S. A. Gorbachenko, N. I. Loginova. - Odesa, 2020. - 148 p.
http://dspace.onua.edu.ua/handle/11300/15973
3. Lisovska Yu. Cyber security. Risks and measures. - K.: Condor, 2019. - 272 p.
http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf
4. 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/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
5. 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/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. 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/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Additional literature:

7. The doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine, version dated 12.30.2021 No. 47/2017. [Electronic resource].
https://zakon.rada.gov.ua/laws/show/47/2017#Text.
8. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine", approved by the Decree of the President of Ukraine, version dated August 26, 2021 No. 447/2021).
https://zakon.rada.gov.ua/laws/show/447/2021#Text
9. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model.
URL: https://www.iso.org/search.html?q=15408-1.
10. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL:
https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
11. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components.
URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
12. ISO/IEC 31010:2019 Risk management . URL:
https://www.iso.org/ru/contents/data/standard/07/21/72140.html
13. 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 Ризик-менеджмент
14. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
15. ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance URL:
https://www.iso.org/ru/contents/data/standard/06/34/63417.html
16. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html

17. ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security. URL: https://www.iso.org/ru/contents/data/standard/07/60/76070.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: 30% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 20% 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