Syllabus
Course Program

Computer networks

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
3

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

General information

Summary

The educational discipline "Computer networks" is a mandatory educational discipline. Network technologies and the Internet affect people in different ways in different countries of the world. In the future, the main directions for developers of new technologies will be related to the use of the Internet as a base for creating new products and services, designed specifically with network capabilities in mind. As developers push the boundaries of what is possible, the capabilities of the interconnected networks that make up the Internet will play an increasingly important role in the success of these projects.

Course objectives and goals

The formation of theoretical knowledge of the basic principles of building modern networks, which include local, global and regional networks, with the help of which new approaches to the management of the modern information society are implemented, as well as the formation of practical skills in the construction and management of corporate systems and networks.

Format of classes

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

Competencies

GC-1. Ability to apply knowledge in practical situations.
GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems.
PC-4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.
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-6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and refusal of various classes and origins.
PC-7. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.).
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-9. Ability to perform professional activities based on the implemented information and/or cyber security management system.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
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 150 hours (5 ECTS credits): lectures - 32 hours, laboratory classes - 32 hours, self-study - 86 hours.

Course prerequisites

Introduction to the specialty. Introductory practice, Physical bases of technical intelligence means, Information security of the state, Legislative foundations of informatization processes in Ukraine, ability to use Linux OS, knowledge of the mechanisms of working with Packet Tracer.

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. Basic provisions of the theory of interaction of open systems.
Chronological succession of important events in the history of the development of computer networks. Chronological succession of important events in the history of the development of computer networks. The general structure of the communication system. Switching methods. Protocols of global networks. Presumptive-temporal characteristics of HVP technologies. Stack of network protocols x.25. Theoretical ways of reducing redundancy. RLE repetitive data compression algorithm. Compression algorithms by KWE keywords. Variable length encoding algorithms. Coding of information in local networks.
Topic 2. OSI model.
Open systems interaction model. Multi-level package nesting system. Enable intermediate network devices. Functions of different iso/osi levels. Transport level. Methods of interaction in the osi/iso network. Functions of different iso/osi levels. Channel level iso/osi. Physical layer (physical layer - pl). Channel level iso/osi. Hardware of local networks. Main functions of adapters. Network adapter driver functions in the osi model. High-level protocols. High-level protocols. Transport protocols. Network protocols. Apple talk stack protocols and the osi/iso model. Classes of networks. Standard network software. Peer-to-peer networks. Server-based networking.
Topic 3. Quality of service QoS.
Basic requirements. Network service quality indicator. Main characteristics of production. Indicators of data transmission quality. Permissible values of the requirements for the main quality indicators. Calculation algorithm. Calculation example.
Topic 4. Methods of retransmission.
Stack of network protocols x.25. A set of hdlc protocols. Method with stop and wait. ARQ with parallel use of virtual channels. Retransmit n steps back. Performance of the ARQ algorithm for N steps back. Transmission with selective repeat. Disadvantages of the method. Methodology for assessing the efficiency of data exchange in the corporate network. Evaluations of the efficiency of data exchange in a corporate network in channels without memory. Performance of various memoryless networks.
Topic 5. Ethernet network.
Ethernet and fast ethernet networks. IEEE 802.X category standards. Types of sublevel LLC procedures. Packet addresses. Address structure. CSMA / CD access method. Emergence of conflict. Combining several cable segments. Evolution of local networks. Functioning of local network switches. Transferring a frame from a port to a switch port. Switching methods. Flow control in half-duplex and duplex modes. Switching technologies and axis model. Three-level hierarchical network model.
Topic 6. Network layer protocol - IP protocol.
Types of addresses. IP address formats. IP Addressing Version 4. IP Header Format . Agreements on special interpretation of IP addresses. Use of masks in IP addressing. Features of IPV6. IPV6 Header . Types of addresses in IPv6. Address representation forms. Addressing model. Allocation of address space. ARP protocol. ARP header structure. Algorithm of using ARP in GVS. Routing in IP networks. Routing tables. DNS protocol. Hierarchy of names in DNS. DNS Record Types . Basic DNS name resolution schemes.

Topic 7. Transport level protocols.
Transport level. Transmission Control Protocol. TCP header. TCP header structure. TCP ports. Establishing a TCP connection. UDP protocol. UDP header. TCP/IP protocol. Level functions. RTP protocol. RTP packet header. RTP-based networks. Sequential inclusion of mixers. RTCP protocol. RTCP report packets. SDES packet format (source description). Characteristics of the source. Checking the correctness of the RTCP header.
Topic 8. Routing protocols.
Routing protocols. Fixed routing. Adaptive routing. Indicators of algorithms (metrics). Routing algorithms. Dynamic routing. To routing. IGP: DISTANCE-VECTOR . IGP: LINK STATE. RIP:Education loops. OSPF (OPEN SHORTEST PATH FIRST).
Topic 9. Modern network technologies.
Network components. Representation and topologies of networks. The main types of networks. Internet connection. Reliable networks. Network security.
Topic 10. Basic configuration of the switch and end device.
IOS navigation. Team structure. Basic configuration of devices. Save changes. Ports and addresses. IP addressing settings.
Topic 11. Protocols and models.
Rules. Protocols. Set of protocols. Organizations for standardization. Reference models. Data encapsulation. Access to data.
Topic 12. Physical level.
Purpose of the physical level. Characteristics of the physical level. Copper cables. UTP cables. Fiber optic cables. Wireless data transmission environment.
Topic 13. Transport level.
Binary number system. Hexadecimal number system. Data transfer. Overview of the TCP protocol. Overview of UDP. Port numbers. The process of data exchange using the TCP protocol. Reliability and flow control. Data exchange using the UDP protocol. Application level, performance level, session level. Peer-to-peer networks. Web traffic and e-mail protocols. IP addressing services. File sharing services.
Topic 14. Principles of network security.
Security threats and vulnerabilities. Network attacks. Protection against network attacks. Device security. Small network devices. Applications and protocols in a small network. Scaling to larger networks. Checking the connection. Host and IOS commands. Troubleshooting methods. Troubleshooting scenarios.
Topic 15. Basic router configuration.
Initial router setup. Settings of interfaces. Default gateway settings.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Study of network tools of joint work.
Topic 2. Study of vacancies in the field of information and network technologies.
Topic 3. Study of services of convergent networks.
Topic 4. Packet Tracer. IOS navigation.
Topic 5. Packet Tracer. Setting the initial parameters of the switch.
Topic 6. Starting the console using the Tera Term program.
Topic 7. Packet Tracer. Creating basic connections.
Topic 8. Creating a simple network.
Topic 9. Setting the switch management address.

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:
CCNA1
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. Information protection technologies./ S.E. Ostapov, S.P. Yevseiev, O.G. King. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf.
2. Yu.V. Volosyuk Computer networks: a course of lectures / Yu. V. Volosyuk. - Mykolaiv: MNAU, 2019. - 203 p.
https://dspace.mnau.edu.ua/jspui/bitstream/123456789/6377/1/Kompiuterni_merezhi_kurs_lektsii.pdf
3. Kurose James F., Ross Keith W. Computer Networking: A Top-Down Approach. 6th Edition / James F. Kurose, Keith W. Ross. - TX: Pearson, 2012. - 864 p.
https://broman.dev/download/Computer%20Networking:%20A%20Top-Down%20Approach%206th%20Edition.pdf
4. CCNAv7: Introduction to Networks course resources [Electronic resource]. – Access mode: https://www.netacad.com/portal/resources/course-resources/ccna-itn.
5. Bonaventure O. Computer Networking: Principles, Protocols and Practice. – Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. – 272 p.
https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf
6. Yevseiev S.P., Ostapov S.E., Korol O.H. Cyber security: modern protection technologies: training. manual for students higher education closing Lviv: "Novy Svit-2000", 2019. - 678 p.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.

Additional literature:

7. Ethernet technology: laboratory workshop / M. O. Bilova, S. P. Yevseiev, O. S. Zhuchenko, I. S. Ivanchenko, O. V. Shmatko.– Lviv: "Novyi Svit-2000", 2020. - 196 p.
https://drive.google.com/drive/u/1/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:
- laboratory work: 20% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- course project: 20% 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