Operating system architecture and security

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 4	**Language of instruction** English

Lecturers and course developers

Serhii POHASII

Serhii.Pohasii@khpi.edu.ua

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

The number of scientific publications: more than 95, including 2 utility model patents, 6 monographs, of which 4 are collective monographs, 4 teaching aids, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 65 articles in foreign publications and specialized publications of Ukraine, with 11 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Analog and digital electronic devices", "Internet of things and services", "Security of cloud technologies", "Fundamentals of construction and protection of modern operating systems", "Modeling of critical infrastructure systems", "Fundamentals of construction and protection of microprocessor systems ", "Security of smart technologies and Internet of things", "Information and communication systems in the field of national security" for undergraduate and graduate students, Section "Information security of cloud services", "Modern methods of protection of socio-cyber-physical systems", "Modeling of mechanisms cyber security" for graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Operating system architecture and security" is a mandatory educational discipline. The discipline is aimed at mastering the principles of using system software, the operating system of a personal computer (server) to maintain it in working condition; knowledge of the basic concepts of the theory of construction of operating systems; prevention of unauthorized access to operating system data; the use of measures against the penetration of malicious software into the environment of the operating system.

Course objectives and goals

Mastering the theoretical foundations of construction, principles of design, configuration and application of various modern operating systems that ensure the organization of computing processes in corporate information systems for economic, management, production, scientific and other purposes, as well as providing practical skills for data protection in modern operating systems.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - 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-4. Ability to identify, state and solve problems in a professional manner.
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.

National Technical University "Kharkiv Polytechnic Institute"

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

Physics, Mathematical foundations of cryptology.

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. Introduction.
Architecture and resources of modern operating systems. Introduction to modern operating systems.
Topic 2. Planning and management of processes and flows.
Processes and flows. Process planning. Process management. Mechanisms of interprocess interaction.
Topic 3. RAM management.
Memory management.
Topic 4. Comprehensive system of data protection of the operating system.
Basics of modern OS protection.
Topic 5. Authentication and management of access to the operating system.
Authentication in SOS.
Topic 6. Account security.
Understanding SUID/SGID. Audit SUID/SGID files. sudo settings. Understanding su. Setting user passwords. Outdated user passwords. Access to network security. File access processes. Setting restrictions for users. View current users. View your login history.
Topic 7. Configuring host security.
Understanding xinetd. Understanding systemd.socket units. Configuring TCP wrappers. Denying access to users. Understanding init. Initialization scripts.
Topic 8. Data protection using encryption.
Understanding OpenSSH. Configuring the OpenSSH client. Authentication and SSH keys. SSH client utilities. SSH tunneling. Understanding GnuPG.

Topics of the workshops

This field is filled in the same way if the curriculum includes workshops

Topics of the laboratory classes

Topic 1. Windows OS deployment on a virtual machine.
Topic 2. Discretionary mechanism for delimiting access to file objects.
Topic 3. Study of processes, threads, descriptors and the Windows registry.
Topic 4. Using Windows PowerShell.
Topic 5. Windows task manager.
Topic 6. Monitoring of system resources in Windows and their management.
Topic 7. The procedure for restoring or resetting a forgotten password.
Topic 8. Analysis of Ethernet frames using the Wireshark program.
Topic 9. Deploying a system for Kali Linux penetration testing.
Topic 10. Security administration.
Topic 11. Extended internet super-server.
Topic 12. Configuring TCP Wrappers.
Topic 13. TCP Wrappers.
Topic 14. Setting the switch management address.

National Technical University
"Kharkiv Polytechnic Institute"

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:
Operating System Basics
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. 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
2. Derrick Rountree, Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Syngress, 211, 2011.
https://books.google.com.ua/books/about/Security_for_Microsoft_Windows_System_Ad.html?id=6kykvSXhkv4C&redir_esc=y
3. Stallings, William. Operating systems: internals and design principles / William Stallings. - 7 th ed. Prentice Hall, New Jersey, 2012, p.769. ISBN-13:978-0-13-230998-1.
4. Kusswurm Daniel. Modern X86 Assembly Language Programming/ Daniel Kusswurm. - Apress, 2019. — 604 p.
https://www.academia.edu/36380133/Daniel_Kusswurm_Modern_X86_Assembly_Language_Programming_32_bit_64_bit_SSE_and_AVX_Apress_2014_
5. Russell S. R., Taylor B. W. Operations management: Creating value along the supply chain. 7 ed. N.-Y. : John Wiley & Sons, Inc., 2010. 832 p.
http://jtelen.free.fr/0MARINE%20bouquins/%5BRoberta_S._Russell,_Bernard_W._Taylor%5D_Operations(Bookos.org).pdf
6. Haseman Chris. Android Essentials / Chris Haseman. - Apress, 2008. - 116 p.
https://books.google.com.ua/books/about/Android_Essentials.html?id=ASmO8r7i93sC&redir_esc=y
7. J. Spealman, K. Hudson, M. Graft, Windows Server 2003: Active Directory Infrastructure. Microsoft Press, pp. 1–8–1–9, 2003.
8. Information protection technologies./ S.E. Ostapov, S.P. Yevseiev, O.G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf

Additional literature:

9. William Stallings. Operating Systems: Internals and Design Principles, 9th Edition. - Pearson, 2018. ISBN-10: 0-13-467095-7 | ISBN-13: 978-0-13-467095-9.
https://books.google.com.ua/books/about/Operating_Systems.html?id=u5M5nQAACAAJ&redir_esc=y
10. Shekhovtsov V. A. Operating systems / V. A. Shekhovtsov – K.: Ed.gr. BHV, 2005. – 576 p.
https://f.eruditor.link/file/2315933/

National Technical University "Kharkiv Polytechnic Institute"

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

28.08.2024   Head of the department
Serhii YEVSEIEV

28.08.2024   Guarantor of the educational program
Serhii YEVSEIEV

Operating system architecture and security

National Technical University "Kharkiv Polytechnic Institute"