Syllabus
Course Program

Administration UNIX-like systems

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
Profile training, Selective

Semester
7

Language of instruction
English

Lecturers and course developers

Andrii TKACHOV
andrii.tkachov@khpi.edu.ua
Candidate of Technical Sciences, senior researcher of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 60 publications, 25 articles in foreign publications and specialized publications of Ukraine, 6 patents for a useful model, guarantor of the educational and professional program of the first (bachelor) level of higher education. Leading lecturer in the disciplines: "Network Programming", "Development and Analysis of Algorithms", "Programming Technologies", "Programming Tools", "Web Security", "Fundamentals of Technical Information Protection", for undergraduate and graduate students.
More about the lecturer on the department's website

Nataliia DZENIUK
nataliia.dzheniuk@khpi.edu.ua
Associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 31, including 2 utility model patents, more than 13 scientific papers.
Specialist in Cisco computer networks, cyber security, Internet of Things, network protection and network intrusion analytics. Leading lecturer in the disciplines: "Security of cloud technologies".
More about the lecturer on the department's website

General information

Summary

The educational discipline "Administration UNIX-like systems" is an optional educational discipline. This course provides basic knowledge of tasks, solution methods and UNIX system administration tools. A wide range of daily tasks of a system administrator is considered: from managing user budgets to installing, configuring, configuring common system components and application software.

Course objectives and goals

Training students to administer UNIX-like systems, show the differences and similar features of a wide range of UNIX systems. The course illustrates the features of various UNIX-like systems: Linux, FreeBSD, Solaris.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control -credit test.

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
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-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
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 120 hours (4 ECTS credits): lectures - 32 hours, laboratory classes - 16 hours, self-study - 72 hours.

Course prerequisites

Basics of programming, Programming technologies.

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. Initial loading and system shutdown.
Initial boot and system shutdown. User accounts.
Topic 2. System kernel loading parameters.
Tuning system kernel boot parameters.
Topic 3. System kernel configuration.

Tuning the parameters of the system kernel.
Topic 4. Terminal access to the system.
Adjusting parameters of terminal access to the system.
Topic 5. Data storage management.
Tuning data storage parameters.
Topic 6. Administration of system services.
Tuning the parameters of system services.
Topic 7. Using the package manager.
Tuning package manager settings.
Topic 8. System security parameters.
Adjusting system security parameters.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Initial loading and system shutdown.
Topic 2. System kernel loading parameters.
Topic 3. System kernel configuration.
Topic 4. Terminal access to the system.
Topic 5. Data storage management.
Topic 6. Administration of system services.
Topic 7. Using the package manager.
Topic 8. Adjusting system security parameters.

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

Course materials and recommended reading

Basic literature:

1. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations Paperback – Illustrated, October 6, 2016.
https://training.epam.ua/ua/blog/564.
2. Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation (Addison-Wesley Signature Series (Fowler)) 1st Edition.
https://proweb.md/ftp/carti/Continuous-Delivery-Jez%20Humble-David-Farley.pdf.
3. Nicole Forsgrenjez, Humblegene Kim: Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations.
https://books.google.com.ua/books/about/Accelerate.html?id=85XHAQAACAAJ&redir_esc=y.

4. Ansible: Up and Running, 2nd Edition by Lorin Hochstein, Rene Moser Released August 2017 Publisher(s): O'Reilly Media, Inc.
https://digtvbg.com/files/LINUX/Meijer%20B.%20Ansible.%20Up%20and%20Running...3ed%202022.pdf.
5. Javascript Tutorial [Електронний ресурс]. – Режим доступу:
https://www.tutorialspoint.com/javascript/index.htm
6. UNIX / LINUX Tutorial [Електронний ресурс]. – Режим доступу:
https://www.tutorialspoint.com/unix/index.htm.
7. WEB technologies [Electronic resource]: Educational reference manual / S.P. Yevseiev, A.M. Tkachov, V.O. Alexeiev, Yu.M. Ryabukha - Kharkiv: KHNEU named after S. Kuznetsia, - Lviv: "New World -2000" Publishing House, 2021. - 390 p.

Additional literature:

1. Tutorials Library [Електронний ресурс]. – Режим доступу:
https://www.tutorialspoint.com/index.htm.

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