Syllabus
Course Program

Cloud 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
Profile, Selective

Semester
6

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 "Cloud security" is an optional educational discipline. The course examines methods and means of ensuring information security and cloud information technologies used for its processing.

Course objectives and goals

Formation of students' knowledge system in the field of classical security techniques for today's cloud security problems. Ensuring the security of web services and solving problems that arise during its improvement. Analysis of the latest cloud security vulnerabilities using standard, systematic methods. Creating your own web service examples and security solutions for them.

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 - 24 hours, laboratory classes - 12 hours, self-study - 84 hours.

Course prerequisites

Antivirus protection of information.

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 to cloud computing.
Subject, purpose and tasks of the discipline. Program learning outcomes. Definition of cloud computing. Characteristics of cloud computing. History and evolution of cloud computing. Advantages and disadvantages of cloud computing. Types of cloud computing. Options for using cloud computing. Cloud

econometrics. Major cloud service providers and their services. Reference architecture of cloud computing.
Topic 2. Elementary basis of cloud computing.
Concept of virtualization. Types of virtualization. Concept of hypervisor. Types of hypervisors. Overview of hypervisors: Hyper-V, VMware, KVM. The concept of a virtual container. Classification of containers. Overview of tools for containerization: OpenVZ, LXC Linux Containers. Overview of the tool for implementing containers on the Linux OS - Docker. Overview of the tool for automating container management (orchestration) - Kubernetes. Java Virtual Machine.
Topic 3. Models of cloud computing.
Infrastructure as a Service (laaS). Platform as a Service (PaaS). Software as a Service (SaaS). Function as a Service (FaaS).
Topic 4. Deployment models of cloud computing systems.
Private cloud (Private Cloud). Public cloud (Public Cloud). Hybrid cloud (Hybrid Cloud). High-performance computing in the clouds (NPC Cloud). Cloud of big data (Big Data Cloud).
Topic 5. Architecture and offers from leading companies providing cloud services.
Microsoft Azure cloud platform. Amazon Web Services cloud platform. Cloud platform IBM Cloud. Google Cloud Platform. Cloud PaaS platform Heroku. Cloud laaS platform DigitalOcean.The local platform as an OpenShift Container Platform service. A complex of free software projects for creating the infrastructure of cloud services and OpenStack storage.
Topic 6. Security in cloud services.
Topic 7. Threats to security in the cloud and proposals for protection against them.
Topic 8. Using the Google Apps cloud service.
Google Drive storage, account, work with tables and documents.
Topic 9. Protection of the Google Apps cloud service.
Creating sites on Google Sites.
Topic 10. Protection of Google Apps cloud service.
Creating a form using Google Forms (advantages of using cloud services to create Internet surveys).
Topic 11. Using SkyDrive cloud environment (Microsoft service).
Creation of surveys (advantages of using cloud services to create Internet surveys).
Topic 12. Cloud-oriented package of Microsoft Office 365 programs and work in it.
Topic 13. Security analysis of Google Apps and Microsoft Office 365 cloud environments.
Topic 14: Deploying a website to Microsoft Azure using Application Services.
Topic 15. Working with relational data in Microsoft Azure.
Topic 16. Cloud technology for creating dynamic Prezi presentations.

Topics of the workshops

Not provided for in the curriculum

Topics of the laboratory classes

Topic 1. Overview of cloud service providers.
Topic 2. Basic models of providing cloud services and their implementation.
Topic 3. Data protection in the clouds.
Topic 4. Google cloud services. Google Docs/Google Drive protection.
Topic 5. Microsoft cloud services. One Drive protection.
Topic 6. Microsoft cloud services. Protecting Microsoft 365 Online.
Topic 7. Setting up the Microsoft Azure development environment.
Topic 8. Microsoft Azure SQL Database Protection.

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 (Cloud Security Fundamentals)
https://paloaltonetworksacademy.net/course/index.php.

Course materials and recommended reading

Basic literature:

1. Bhowmik S. Cloud Computing. Delhi : Cambridge University Press, 2017. 434 p. https://books.google.com.ua/books/about/Cloud_Computing.html?id=jeTFDgAAQBAJ&redir_esc=y.
2. Cloud Computing : Principles, Systems and Applications I Editors Nick Antonopoulos and Lee Gillam; second ed. Swindon : Springer International Publishing AG, 2017.410 p. https://download.e-bookshelf.de/download/0009/9634/13/L-G-0009963413-0020076340.pdf.
3. Collier M., Shahan R. Microsoft Azure Essentials - Fundamentals of Azure / second ed. Redmond : Microsoft Press, 2016. 250 p. https://books.google.com.ua/books/about/Microsoft_Azure_Essentials_Fundamentals.html?hl=el&id=EfFxBgAAQBAJ&redir_esc=y.
4. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P. https://books.google.com.ua/books/about/The_Internet_of_Things.html?id=oyyyBwAAQBAJ&redir_esc=y.
5. Aulov I.F., Study of the model of intrusions of key cloud systems and proposals for protection against them. Eastern European Journal of Advanced Technologies 5/2 (77) 2015, ISSN 1729-3774, DOI: 10.15587/1729-4061.2015.50912, - P.13. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vej_pte_2015_5(2)__2.
6. Voytovych N.V., Naidyonova A.V. The use of Google cloud technologies and web 2.0 services in the educational process. Methodical recommendations. - Dnipro: DPTNZ "Dniprovsky center of PTOTS", 2017 - 113 p. https://online.fliphtml5.com/arbd/jejq/#p=1.

Additional literature:

7. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P. https://dl.matlabyar.com/siavash/ML/Book/Ethem%20Alpaydin-Introduction%20to%20Machine%20Learning-The%20MIT%20Press%20(2014).pdf.
8. C Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.

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

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV