COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cloud security mechanisms and principles [S2Teleinf2-SDP>BwC]

Course

Field of study
Teleinformatics

Year/Semester
2/3

Area of study (specialization)
Software-defined systems

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
14

Laboratory classes
24

Other
14

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Lecturers

Prerequisites

A student starting this course should have a basic knowledge of, ICT networks, operating systems, cloud systems and have basic programming skills. He/she should also have the ability to obtain information from the indicated sources. The student should demonstrate qualities such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for others and willingness to work in a group.

Course objective

11 To provide students with theoretical background on cloud systems. 2. To familiarise students with theoretical information on the security of cloud systems infrastructure. 3. To familiarise students with basic information on security management of cloud systems and risk estimation. 4. To familiarise students with basic information on data security in cloud systems. 5. To familiarise students with the basic concepts of cloud security operations and identity and access management.

Course-related learning outcomes

Knowledge:
He/she has an expanded and in-depth knowledge in the following area of modern data transmission and processing systems, especially cloud systems [K2_W02]
Is familiar with and comprehends advanced artificial intelligence methods applied in designing teleinformatics systems and information processing in teleinformatics systems [K2_W04]
Understands the methodology of designing complex teleinformatics systems; familiar with hardware description languages and computer-aided design and simulation tools for cloud systemsK
Has knowledge of developmental trends and significant new achievements in the field of cloud computing [K2_W07]

Skills:
He/she is able to acquire information from literature, databases, and other sources; integrate the obtained information; interpret and critically evaluate it; draw conclusions; and formulate and thoroughly justify opinions [K2_U01]
Can propose improvements or alternative solutions for existing design solutions and teleinformatics systems in cloud computing area [K2_U09]
Can assess the usefulness and feasibility of incorporating new advancements in technical techniques and design methods for creating innovative solutions in the design and production of teleinformatics systems in cloud computing area [K2_U10]

Social competences:
Is ready to recognize the significance of knowledge in solving cognitive and practical problems and to critically evaluate received content [K2_K01]
Is ready to think and act in an entrepreneurial manner [K2_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: Knowledge is verified by a written and/or oral test consisting of 3-5 questions. The pass mark is 51% and no support material is allowed during the test
Laboratory: Knowledge is verified on an ongoing basis during the laboratory activities on the basis of reports and through a colloquium and/or project defence at the end of the semester. The passing grade is 51% of the points, and no supporting materials may be used during the test except those provided by the lecturer.

Programme content

Lecture topics:
- introduction to cloud systems
- security of infrastructure in cloud systems
- communication security in cloud systems
- data security in cloud systems
- security and risk management in cloud systems
- Cloud Security Operations
- penetration testing, auditing and security analysis of cloud systems
- virtualisation and applications in cloud systems

Lab topics:
consistent with the topics of lectures

Course topics

Lecture topics:
- introduction to cloud systems
- security of infrastructure in cloud systems
- communication security in cloud systems
- data security in cloud systems
- security and risk management in cloud systems
- Cloud Security Operations
- penetration testing, auditing and security analysis of cloud systems
- virtualisation and applications in cloud systems

Lab topics:
consistent with the topics of lectures

Teaching methods

Lecture: multimedia presentation, illustrated by examples given on the blackboard and practical demonstrations.
Laboratory exercises: practical exercises carried out alone or in groups using a computer.

Bibliography

Basic:
Chris Dotson, Bezpieczeństwo w chmurze, Wydawnictwo Naukowe PWN, 2020
Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Additional:
P. Mishra, E. S. Pilli, R. C. Joshi, “Cloud Security: Attacks, Techniques, Tools, and Challenges”, CRC Press.,
2021 (https://www.amazon.com/Cloud-Security-Attacks-Techniques-Challenges-ebook/dp/B09MTT5D3T)
J. R. Vacca, “Cloud Computing Security: Foundations and Challenges”. CRC Press, 2016 (https://www.amazon.com/Cloud-Computing-Security-Foundations-Challenges/dp/1482260948)
C. Dotson, “Practical Cloud Security: A Guide for Secure Design and Deployment”, O'Reilly Media, 2019 (https://www.amazon.com/Practical-Cloud-Security-Secure-Deployment/dp/1492037516)

Breakdown of average student's workload

	Hours	ECTS
Total workload	103	4,00
Classes requiring direct contact with the teacher	38	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	65	2,50