# COURSE DESCRIPTION CARD - SYLLABUS

Course name
Mechanisms of violations and ensuring security in cloud and DC

## Course

Field of study
Computing

Year/semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
English

Form of study
full-time

Requirements
elective

## Number of hours

| Lecture | Laboratory classes | Other (e.g. online) |
|---|---|---|
| 15 | 30 | |
| Tutorials | Projects/seminars | |

## Number of credit points

4

## Lecturers

Responsible for the course/lecturer:
dr inż. Marek Michalski
marek.michalski@put.poznan.pl
tel: 61 665 39 06
Faculty of Computing and Telecommunications

Responsible for the course/lecturer:

## Prerequisites

Student has basic knowledge and experience about PC, virtualization, computer networks, IP protocols (including routing) and programming

## Course objective

To show to students problems with security where cloud services are realized and data center is operated

## Course-related learning outcomes

Knowledge

The student understands the mechanisms that are used during the implementation of services in clouds and data centers, student is aware of their weaknesses and how to improve their security

Skills

The student is able to analyze the cloud system and data center, indicate possible threats and correlate the way of eliminating them

Social competences

Student understands that in the field of security his knowledge and skills very quickly become obsolete.

## Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Written test, 51% to pass

## Programme content

Basics of building clouds and cloud services

Technical and non-technical aspects of cloud services I

mplementation of selected services on examples from Google, MS, AWS and others

Tools and techniques for implementing cloud services

Mechanisms of security breaches Danger areas

Protection mechanisms and the possibility of their automation

Tools for operators, service providers and customers

Examples of sources of disclosed problems

DC General Building, DC Services and Mechanisms

Principles of virtuality, Characteristics of clients

Mechanisms of occurrence of security breaches in DC

Threat categorization, command-and-control (C&C)

Mechanisms of defense against threats and their automation

Custom hardware for data Center (FPGA, option)

The lecture will include a visit to two (or more) data centers in Poznań, And also a meeting with people who work with security tools on a daily basis (security systems integrator) and companies providing services in the field of testing and increasing the level of security (companies from the local market and a well-known nationwide portal dealing with IT security)

Lab

Practical familiarization with the test sample Cloud and Data Center environment

Virtualization of operating systems, computer networks and their functionalities (VM, NFV)

Getting to know typical WAF solutions, threat detection / threat protection tools, IDS / IPS (Intrusion Detection Systems / Intrusion Protection Systems)

Discovery of command-and-control (C&C) mechanisms

## Teaching methods

Lecture with elements of discussion with students, demonstrations

Lab with experiments on real network, example of cloud and data centers

## Bibliography

Basic

Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Additional

## Breakdown of average student's workload

| | Hours | ECTS |
|---|---|---|
| Total workload | 100 | 4,0 |
| Classes requiring direct contact with the teacher | 45 | 2,0 |
| Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) [1] | 55 | 2,0 |

[1] delete or add other activities as appropriate