Course title: Protection of Computer Systems

Teacher(s): Marjan D. Milošević

Course status: elective

Number of ECTS credits: 10

Condition: None

Course objectives

Introduction of modern features of computer systems' protection. Upgrading previously acquired knowledge in the field of data protection and security of networked systems. Introducing to research methodology in the area of information-communication systems security.

Learning outcomes

The student is capable of analysing threats and modern protection methods on various levels (application, operating systems, network infrastructure). Student individually models threats in the Internet of Things and Cloud Computing environment.

The student can use knowledge sources in the area of information security and upgrade existing concepts and solutions. The student can apply current programming paradigms to develop protection solutions and protection mechanism assessments. The student applies scientific methodology in the research of computer systems protection.

Contents

Theoretical lectures

Security policies and mechanisms. Standardisation. Perimeter security. Cryptography-based protection methods. Security protocols. Zero-knowledge. Security of networked systems, Internet of things and cloud. Advanced intrusion detection methods. Anonymity and privacy protection. Blockchain application in computer system protection. Usability of the protection software and systems. Review of the latest results in the research of the area.

Practical lectures

Teaching is partly implemented via individual research in the area of information security. Research study work involves active studying of scientific literature, design of protection systems, organisation and conducting of measurement and testing, data collection and processing, and writing scientific papers in the area of information security.

Recommended literature

[1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, Indianapolis, 2020

[2] M.H. Bhuyan, D. K. Bhattacharyya, J.K. Kalita, *Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools*, Springer International Publishing AG, Cham, 2017.

[3] Martin K., *Everyday Cryptography Fundamental Principles and Applications*, Oxford University Press, Oxford, 2017

[4] Scientific journals (Computers and Security, Journal of Information Security and Applications, IEEE Security and Privacy, ACM Transactions on Privacy and Security…)

Number of active classes: 7	Theory: 5	Practice: 2

Teaching methodology

Presentation, case study, practical work, study research work

Evaluation (maximum number of points 100)

Ways of testing the knowledge:
Homework- 20
Project - 30
Oral exam- 50

*maximum length 1 A4 page