COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security in Computer Systems

Course

Field of study
Computing

Year/Semester
2/3

Area of study (specialization)
IT in Business Processes

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
Polish

Form of study
part-time

Requirements
compulsory

Number of hours

Lecture
16

Laboratory classes
16

Other (e.g. online)

Tutorials

Projects/seminars

Number of credit points

4

Lecturers

Responsible for the course/lecturer:
dr inż. Tomasz Łukaszewski

Responsible for the course/lecturer:
mgr inż. Bartosz Zgrzeba

Prerequisites

The student starting this course should have basic knowledge of computer networks, operating systems, internet applications and security of information systems. He should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of the team.

Course objective

Provide students with an extended knowledge of computer systems and the Internet of Things in the field of security of these systems. Developing students' skills in solving problems related to security in computer systems and the Internet of Things.

Course-related learning outcomes

Knowledge

1. Has ordered, theoretically founded general knowledge in the field of operating systems and network technologies 2. Has theoretically founded detailed knowledge related to selected issues in the field of computer science, such as: security of information systems and the Internet of Things 3. Has knowledge of development trends and the most important new achievements in information technology in the field of data protection and security of computer systems

Skills

1. Is able to use the services available in computer systems and the Internet of Things, taking into account the security aspect. 2. Is prepared to use in professional work the components of computer systems and the Internet of Things in a way that takes into account the security of the solutions created.

Social competences

Understands that knowledge and skills become obsolete very quickly in computing

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired during the lecture is verified by a written exam. The exam consists of approximately 30 questions (closed). Passing threshold: 50% of points. The completion of the questions will be sent to students before the exam. The skills acquired during the laboratory classes are verified on the basis of the presentation of the project consisting in the analysis of the indicated problem related to security in the Internet of Things.

Programme content

The lecture program covers the following topics:

1. Introduction to security issues: defining the concept of hacking, analyzing the operation of malicious programs, defining the concepts of security, threats, vulnerabilities and attacks. Presentation of current security initiatives.

2. Legal issues related to the use of computer systems: computer piracy, copyright infringement, infringement of personal rights and others.

3. Password security (threats related to the use of password types) and Biometrics (application in the authentication process).

4. Security of electronic services: electronic banking, electronic commerce.

5. Security of payment cards, RFID technology, cryptocurrencies.

6. Privacy and anonymity in computer systems.

7. Security of cyberspace and social media.

8. Threats: spam, phishing, spyware, phishing, stalking, scam.

9. Attacks: SSL strip, Clickjacking, HTTP Session hijacking

10. WiFi network security: analysis of the vulnerabilities of WEP, WPA, WPA2 mechanisms.

The laboratory program covers the issues discussed during the lectures. In addition, at the last laboratories, students defend the project - they discuss the results of the analysis of the problem related to security in computer systems and the Internet of Things.

Teaching methods

lecture: multimedia presentation, demonstration of examples of threats and methods of defense

laboratory exercises: practical exercises, discussion, team work, analysis of multimedia materials

Bibliography

Basic

1. Viega J., Mity bezpieczeństwa IT, Helion, 2010

2. Strebe M., Podstawy bezpieczeństwa sieci, Mikom, 2005

3. Sikorski M., Roman A. M., Internet rzeczy, PWN 2020

Additional

1. Zalewski M., Cisza w sieci, Helion, 2005

2. Zalewski M., Splątana sieć, Helion, 2012

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,0
Classes requiring direct contact with the teacher	37	2,0
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) [1]	63	2,0

[1] delete or add other activities as appropriate