Module/Course Syllabus
Program: COMPUTER SCIENCE
Full-time master degree program

Course:	**Security in computer networks**
Type of the course:	directional
Course code:	I2S1.07
Year:	I
Semester:	1
Form of the degree program:	full-time
Form of classes and number of hours per semester:	60
Lecture	30
Classes	0
Laboratory	30
Project	0
Number of ECTS credits:	4
Form of assessment:	exam
Course language:	English

Course objective (CO)	
CO1	Familiarize students with the security of the computer network and operating system.
CO2	Acquisition of skills by students to effectively detect and prevent threats using appropriate techniques.

Prerequisites in terms of knowledge, skills and other competencies	
1	Knowledge of the operation of computer networks.
2	Knowledge of network operating systems configuration.

Learning outcomes (LO)	
	In terms of knowledge:
LO 1	Has knowledge of monitoring and detecting various network attacks.
LO 2	Has structured knowledge of selected tools for monitoring network protocols and services.
LO 3	Has knowledge of selected tools for monitoring network protocols and services.
	In terms of skills:
LO 4	Is able to configure and monitor selected operating systems in terms of network security.
LO 5	Can detect and correctly identify selected types of attacks in various network infrastructures.
LO 6	Can plan and organize testing of network security, systems and network services.
	In terms of social competence:
LO 7	Can critically assess his knowledge related to attacks on network infrastructure.

Course content	
Form of classes – lectures (L)	
	Course content
L1	Basic tasks of security and cybersecurity in network infrastructure.
L2	The function and characteristics of the Windows operating system required for the analysis of security in a computer network.

L3	The function and characteristics of the Linux operating system required for security analysis in a computer network.
L4	Fundamentals of network protocols and services analysis.
L5	Presentation of the principles of communication in the network infrastructure.
L6	Classification of different types of network attacks.
L7	Methods of detection and protection against attacks in layer II of the OSI model.
L8	Methods of detection and protection against attacks in layer III of the OSI model.
L9	Presentation of tools for identifying attacks on network protocols and services.
L10	Methods of preventing unauthorized access to hardware and software resources.
Form of classes – laboratories (Lab)	
	Course content
Lab1	Preparation of the environment for monitoring and detecting network attacks.
Lab2	Monitoring and securing the Windows operating system.
Lab3	Monitoring and securing the Linux operating system.
Lab4	Methods of detection and protection against attacks in layer II of the OSI model
Lab5	Methods of detection and protection against attacks in layer III of the OSI model
Lab6	Methods of detection and protection against attacks in layers IV-VII of the OSI model.
Lab7	Methods of detection and protection against attacks in wireless networks.
Lab8	Methods of detection and protection against attacks on network services.
Lab9	Methods of encrypting data sent in the network infrastructure.
Lab10	Configuration of methods to prevent unauthorized access to hardware and software resources.

Didactic methods	
1	Lecture with multimedia presentation.
2	Subject discussion.
3	Performing the exercises.

Assessment methods and criteria		
Assessment method symbol	**Assessment method description**	**Passing threshold**
A1	Lecture exam	51%
A2	Laboratory pass	51%

Required textbooks and other course materials	
1	Cole E., Network Security Bible 2nd Edition, Wiley & Sons, 2009.
2	Singer W. P., Friedman A., Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014.
3	White K. A., Hacking: The Underground Guide to Computer Hacking, Including Wireless Networks, Security, Windows, Kali Linux and Penetration Testing, 2017
Recommended textbooks and other course materials	
1	Banasiński C., Cyberbezpieczeństwo. Zarys wykładu, Helion, 2018
2	Janczuk M., Sawicki D., Analysis of the possibilities of using IPSec on a Linux system for wireless networks, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, 2018

Student workload	
Form of activity	**Average number of hours to complete the activity**

Contact hours with the lecturer, including:	60
participation in lectures	30
participation in laboratories	30
Student's own work, including:	40
preparation for the exam	20
preparation for the laboratory	20
Total student workload	100
Total number of ECTS credits	4

Learning outcomes matrix					
Learning outcome	**Reference to learning outcomes defined for the master's program**	**Course objectives**	**Course content**	**Didactic methods**	**Assessment methods**
LO 1	I2A_W01 + I2A_W04 + I2A_W08 ++	CO1	L1, L4 –L6, L9	1	A1
LO 2	I2A_W04 ++ I2A_W08 +	CO1	L2, L3, L7, L8, L10	1	A1
LO 3	I2A_W08 +	CO1	L1, L5, L9	1, 2	A1
LO 4	I2A_U15 ++	CO2	Lab1 – Lab3, Lab7, Lab8	3	A2
LO 5	I2A_U15 + I2A_U16 +++	CO2	Lab4 - Lab8	2, 3	A2
LO 6	I2A_U15 + I2A_U16 +	CO2	Lab2 – Lab8	2, 3	A2
LO 7	I2A_K01 +	CO2	Lab8 – Lab10	3	A2

The author of the program:	dr inż. Daniel Sawicki
E-mail address:	d.sawicki@pollub.pl
Organizational unit:	Department of Electronics and Information Technology