Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

COURSE DESCRIPTION

Course code	full-time studies	
	part-time-studies	
Course name	**Zaawansowane zagadnienia cyberbezpieczeństwa**	
Course name in English	**Advanced cybersecurity solutions**	
Valid from academic year	**2022/23**	

PLACEMENT IN THE TEACHING PROGRAM

Field of study	**Computer Science**
Level of education	**1st degree**
Studies profile	**General**
Form and method of teaching classes	**Full-time and part-time studies**
Specialization	**Information and communication technology**
Organizational unit responsible for the course	**Katedra Systemów Informatycznych**
Course coordinator	**dr inż. Mirosław Płaza**
Approved by	**Dean of the Faculty of Electrical Engineering, Automatic Control and Computer Science Roman Deniziak, KUT prof., DSc, PhD**

GENERAL CHARACTERISTIC OF THE COURSE

Course affiliation		**Speciality**
Course status		**not obligatory**
Language		**English**
Semester	full-time studies	**Semester VII**
	part-time-studies	**Semester VIII**
Requirements		**Computer networks, Routing and Switching Essentials, Cybersecurity**
Exam (YES/NO)		**NO**
ECTS		**6**

Course form		**lecture**	**classes**	**laboratory**	**project**	**other**
Hours per semester	full-time studies	**30**		**30**	**15**	
	part-time-studies	**18**		**18**	**9**	

LEARNING RESULTS

Category	Result Symbol	Learning Results	References to the field of study results
Knowledge	W01	Students know and understand advanced methods of security monitoring in ICT systems.	INF1_W32
	W02	Students know and understand methods for enhancing security in defined cyberspaces.	INF1_W32
	W03	Students know and understand the vulnerabilities of ICT systems.	INF1_W32
Skills	U01	Students can design complex ICT systems with an eye to ensuring protection from threats.	INF1_U32
	U02	Students can solve complex cybersecurity problems.	INF1_U32
	U03	Students can identify the needs for the use of cybersecurity techniques.	INF1_U32
Social competence	K01	Students are prepared to continuously update their knowledge in the field of cybersecurity.	INF1_K1 INF1_K2
	K02	Students are prepared to evaluate cybersecurity issues and their effects on society.	INF1_K1 INF1_K2

COURSE CONTENT

Course Form	Content
lecture	1. **Cybersecurity issues in IoT solutions** (vulnerability and risk assessment in IoT systems, IoT security issues in device layer, communication layer and application layer). 2. **Advanced security issues in operating systems** (Windows, Linux). 3. **Network security systems** (deployed on a host, in an IoT network infrastructure or in the cloud using examples of Firewall, IPS, AMP class solutions). 4. **Advanced methods of reducing the impact of malware** (security monitoring, analysis of data used in security monitoring systems, security incidents). 5. Impact of encryption algorithms and secure communication protocols as well as hash functions on security. 6. **Advanced security solutions for cloud infrastructure** (infrastructure security, application security, secure cloud management).
laboratory	1. Cybersecurity of IoT – vulnerability testing and analysis of IoT applications and devices. 2. Advanced security issues in Windows operating system. 3. Advanced security issues in Linux operating system. 4. Exploration of advanced features of network analyzers in assessing vulnerabilities of various network protocols. 5. Investigating the possibility of attacks on selected database types. 6. Encryption and decryption of data using selected methods. 7. Advanced security incident handling procedures. 8. Advanced cybersecurity techniques in the cloud computing area.

project	Topics of project assignments include: • literature analysis of existing solutions to a given engineering problem, • analysis and selection of appropriate techniques for effective implementation of the given problem with justification of the choices made, • design of the system/task under development, along with a description of the techniques and tools used, • preparation of project documentation, which describes in detail the executed project along with the project assumptions – the documentation is prepared independently by the team implementing the project, • description of how to implement the developed solution along with the user manual, • analysis of further development possibilities of the prepared solution, • presentation of the developed solution.

LEARNING RESULTS VERIFICATION METHODS

Result Symbol	Learning results verification methods					
	Oral Exam	Written Exam	Midterm	Project	Report	Other
W01			X			
W02			X			
W03			X			
U01			X			
U02			X			
U03			X			
K01			X			
K02			X			

ASSESSMENT FORMS AND CRITERIA

Course Form	Assessment Form	Assessment Criteria
lecture	pass with a grade	Obtaining at least 50% of the points from the pass tests during the laboratory classes.
laboratory	pass with a grade	Obtaining at least 50% of the points from the pass tests during the laboratory classes.
project	pass with a grade	Defense of projects prepared.

STUDENT’S VOLUME OF WORK

ECTS Balance												
No.	Activity Type	Student Involvement										Unit
		full-time studies					part-time-studies					
1.	Participation in classes according to the schedule	Lec	C	Lab	P	S	Lec	C	Lab	P	S	h
		30		30	15		18		18	9		
2.	Other (consultations, exams)	2		2	2		2		2	2		h
3.	**Total with the direct assist of an academic teacher**	**81**					**51**					h
4.	**Number of ECTS, that students obtains with the direct assist of an academic teacher**	**3,24**					**2,04**					ECTS

5.	**Hours of unassisted student work**	**69**	**99**	h
6.	**Number of ECTS that student obtains working unassisted**	**2,76**	**3,96**	ECTS
7.	**Practical classes volume of work**	**45**	**27**	h
8.	**Number of ECTS obtained by student at practical classes**	**1,80**	**1,08**	ECTS
9.	**Total student's volume of work expressed in hours**	**150**	**150**	h
10.	**ECTS**	**6**		

BIBLIOGRAPHY

1. Omar Santos, **Cisco CyberOps Associate Official Cert Guide**, 2020
2. Cisco Networking Academy, **CCNA Cybersecurity Operations Companion Guide**, 2018