Politechnika Świętokrzyska

WYDZIAŁ ELEKTROTECHNIKI, AUTOMATYKI I INFORMATYKI

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	**Wybrane aspekty cyberbezpieczeństwa**	
Course name in English	**Selected aspects of cybersecurity**	
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 systems**
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		**obligatory**
Language		**English**
Semester	full-time studies	**Semester VII**
	part-time-studies	**Semester VIII**
Requirements		**Computer networks**
Exam (YES/NO)		**TAK**
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 contemporary cybersecurity issues.	INF1_W32
	W02	Students know and understand the solutions to design / run security services in the ICT network.	INF1_W32
	W03	Students know and understand architecture, organization and security solutions for operating systems.	INF1_W32
Skills	U01	Students are able to match the appropriate level of security to ensure protection against threats.	INF1_U32
	U02	Students are able to design / run / test a security service in an ICT network.	INF1_U32
	U03	Students are able to plan and carry out experiments on protection of resources available through ICT networks.	INF1_U32
Social competence	K01	Students are prepared to assess the importance of cybersecurity in today's world.	INF1_K1 INF1_K2
	K02	Students are prepared to work and collaborate in a group in the field of creating security in the field of ICT.	INF1_K1 INF1_K2

COURSE CONTENT

Course Form	Content
lecture	1. **Introduction to cybersecurity issues** (cyberspace, cybercrime; types of vulnerabilities). 2. **Threats, vulnerabilities and attacks in the cyber world** (malware and advanced protection mechanisms; DoS, DDoS attacks and how to respond to them). 3. **Selected types of attacks** (access attacks; attacks on network infrastructure and services; attacks on wireless networks). **4. Data theft prevention systems.** 5. **Cloud computing** (basic cybersecurity solutions operating in cloud computing). 6. **Security systems design** (principles of security systems design and evaluation; information systems security policy). **7. Selected legal aspects in the area of cybersecurity.** **8. Cybersecurity issues in IoT solutions** (vulnerability and risk assessment in IoT systems, security issues in different layers of IoT systems reference model). 9. **Selected security issues in operating systems** (Windows, Linux)
laboratory	1. Data protection in the cyber world – data integrity testing. 2. Virtual machine security. 3. Detection of threats and vulnerabilities in ICT security. 4. Attacks on desktop and mobile devices. 5. Examining traffic between client and remote website. 6. Basic VPN tunnel configuration. 7. User passwords recovery using system tools. 8. Testing and basic configuration of firewall. 9. Access control lists in cybersecurity issues. 10. Cybersecurity of IoT – vulnerability testing and analysis of IoT applications and devices. 11. Security in operating systems.

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	exam	Obtaining at least 50% of the points during the exam.
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. Charles J. Brooks, Donald Short, Christopher Grow, **Cybersecurity Essentials**, 2018
2. Omar Santos, **Cisco CyberOps Associate Official Cert Guide**, 2020
3. Cisco Networking Academy, **CCNA Cybersecurity Operations Companion Guide**, 2018