Zał. nr 5 do ZW 16/2020

Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Złośliwe Mechanizmy i Techniki Ochrony**
Name of the course in english	:	**Malicious Mechanisms and Defence Techniques**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	W04INA-SM4119G
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	90		90		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	3		3		
including the number of points corresponding to the classes of practical (P)			3		
including the number of points corresponding occupations requiring direct contact (BK)	2		2		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

knowledge of issues from the lecture on cryptography and algebraic number theory

COURSE OBJECTIVES

C1 acquiring knowledge and skills in the field of hostile software/hardware and methods of protection against it

C2 practical skills in implementing security countermeasures

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 understands the mechanisms used in the basic areas of operation of hostile IT products

W2 knows the mechanisms of preventing threats in the most important areas of attacks

W3 knows the mechanisms of protection against black box solutions

The student skills:

U1 is able to locate potential vulnerabilities and their determinants

U2 is able to design and implement protection using standard technical means

U3 is able to design and implement innovative protection mechanisms

The student's social competence:

K1 understands the mechanisms of social engineering and the attacks resulting from it

K2 is able to implement IT projects in a user-friendly and transparent manner

COURSE CONTENT

Type of classes - lectures		
Wy1	computer viruses and worms	2h
Wy2	attacks on password systems	2h
Wy3	security issues in P2P systems	4h
Wy4	web security	2h
Wy5	algorithms of distributed attacks	2h
Wy6	spam filtering	2h
Wy7	security problems of mobile devices	2h
Wy8	security mechanisms for IoT devices	4h
Wy9	subversion resilience mechanisms	2h
Wy10	watchdog mechanism	2h
Wy11	PUF	2h
Wy12	high level cryptographic protection	4h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	tools for detecting and analyzing viruses, worms	2h
Lab2	attacking password systems	2h
Lab3	chosen P2P systems and studying their vulnerabilities	2h
Lab4	Web site vulnerabilities and security tools	4h
Lab5	defence against DDoS attacks	2h
Lab6	configuration of spam filtering	2h
Lab7	security mechanisms of Android	2h
Lab8	security design of smart meters	2h
Lab9	cryptographic protocols for protection against clones and loss of control over the device	4h
Lab10	protocols eliminating hidden channels	4h
Lab11	application of PUF mechanisms	2h
Lab12	emerging topics	2h
	Sum of hours	30h

Applied learning tools
1. Multimedia lecture 2. Solving tasks and problems 3. Solving programming tasks 4. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS		
Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K2	tests
F2	U1-U3, K1-K2	
P=50%*F1+%*F2		

BASIC AND ADDITIONAL READING
1. Lecture Notes on “Computer and Network Security”, Avi Kak, Perdue Univ.

SUPERVISOR OF COURSE
prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Złośliwe Mechanizmy i Techniki Ochrony
WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

Subject learning effect	Relating the subject effect to the learning outcomes defined for the field of study	Objectives of the course**	Program content**	Teaching tool number**
W1	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy12	1 4
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy12	1 4
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W09 K2_W10	C1	Wy1-Wy12	1 4
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab12	2 3 4
U2	K2_U01 K2_U02 K2_U03 K2_U05 K2_U06 K2_U07 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab12	2 3 4
U3	K2_U01 K2_U02 K2_U03 K2_U05 K2_U06 K2_U07 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab12	2 3 4
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K11 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab12	1 2 3 4
K2	K2_K01 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab12	1 2 3 4