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	:	**Uczenie maszynowe i bezpieczeństwo**
Name of the course in english	:	**Machine Learning and Security**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4121G`
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		
Assesement	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

COURSE OBJECTIVES

C1 Presentation of the application of machine learning (ML) to anomaly and threat detection in information systems. Overview of ML based network attacks detection. Presentation of the basic threats related to the ML process. Discussion of techniques ensuring the integrity of the inputs and outputs of the ML process. Overview of mechanisms ensuring the privacy and confidentiality of machine learning implemented on remote platforms. Discussion of the problem of provable remote training in ML processes.

C2 Implementation of selected anomaly detection techniques based on machine learning (ML). Practicing the implementation of selected methods that ensure privacy and confidentiality of ML processes.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 ML usage in anomaly and threats detection

W2 Awareness of threats and vulnerabilities related to ML processes

W3 Protection of ML processes

The student skills:

U1 can detect ML related anomalies and threats

U2 can identify threats and vulnerabilities related to ML processes

U3 can design and manage protection of ML processes

The student's social competence:

K1 can determine the security of solutions based on machine learning in the economic and social context

K2 can identify potential pragmatic application areas for machine learning

COURSE CONTENT

Type of classes - lectures		
Wy1	introduction to ML	4h
Wy2	ML based anomaly and threats detection	4h
Wy3	ML in Cloud	4h
Wy4	data Secrecy in ML	3h
Wy5	privacy in ML	3h
Wy6	training data injection, poisoning and mislabeling	3h
Wy7	secure Federated ML	3h
Wy8	secure ML using Homomorphic Encryption	3h
Wy9	proof of learning, proof of training	3h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	introduction to ML	6h
Lab2	ML based anomaly and threats detection	6h
Lab3	training data injection, poisoning and mislabeling	6h
Lab4	privacy and secrecy in ML	6h
Lab5	proof of learning, proof of training	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Solving programming tasks
3. Creating programming projects
4. Consultation
5. 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	
F2	U1-U3, K1-K2	Average of partial grades for solved lists of laboratory tasks.
P=%*F1+1%*F2		

BASIC AND ADDITIONAL READING

1. The literature will be given at the beginning of the class by the lecturer

SUPERVISOR OF COURSE

dr hab. inż. Łukasz Krzywiecki

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Uczenie maszynowe i bezpieczeństwo

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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy9	1 4 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 4 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W09 K2_W10	C1	Wy1-Wy9	1 4 5
U1	K2_U01 K2_U02 K2_U04 K2_U05 K2_U06 K2_U07 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	2 3 4 5
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	2 3 4 5
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	2 3 4 5
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy9 Lab1-Lab5	1 2 3 4 5
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy9 Lab1-Lab5	1 2 3 4 5