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	:	**Procedury i Bezpieczeństwo Operacyjne**
Name of the course in english	:	**Compliance and Operational Security**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4001G`
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)	60	60			
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	2	2			
including the number of points corresponding to the classes of practical (P)		2			
including the number of points corresponding occupations requiring direct contact (BK)	2	2			

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Knows the basics of cryptology and computer security.

COURSE OBJECTIVES

C1 Presentation of the principles of a design and maintenance of an information security system in an enterprise or an institution.

C2 Teaching students the rules of creating documentation for an information security system.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows rules of risk analysis

W2 Knows legal, economical, and social aspects influencing security policies

W3 Knows vital normative and legal requirements for information security

W4 Knows concepts, architectures and roles of Security Information and Event Management (SIEM) and Security Operation Center (SOC)

W5 Knows basics principals of personal data protection stated by GDPR

W6 Knows concept of open banking and fundamental standards applies to the financial market - PSD2, RTS, PCI DSS

W7 Knows concept and rules of standardization of Common Criteria (CC)

The student skills:

U1 Is able to further develop her/his competences by reading standards, best practices and legal acts.

U2 Is able to correctly estimate impact and costs of security solutions proposed.

U3 Is able to see limitations of the methodology of information security management.

The student's social competence:

K1 Has competences in the design and implementation of security training.

K2 Can use project management techniques with respect to duties of security administrators.

K3 Able to perform tasks in a pragmatic and creative way.

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to cybersecurity issues, evet and incident definition, monitoring and logging	2h
Wy2	Security Information and Event Management (SIEM) and Security Operating Center (SOC)	2h
Wy3	Risk related concepts	2h
Wy4	Risk mitigation strategies	4h
Wy5	Incident response procedures	4h
Wy6	Security awareness	2h
Wy7	Business continuity	2h
Wy8	Environmental controls	2h
Wy9	Essentials of personal data protection defined by GDPR	2h
Wy10	Open baking and financial market standards - PSD2, RTS, PCI DSS	4h
Wy11	Disaster Recovery	3h
Wy12	The AIC (Availability, Integrity, Confidentiality) triad	1h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Analysis of selected Security Information and Event Management (SIEM) system	4h
Ćw2	Risk analysis.	4h
Ćw3	Analysis of selected case studies in terms of GDPR compliance	4h
Ćw4	Security policy, security plan and documented operating procedures.	6h
Ćw5	Incident response procedures.	6h
Ćw6	Contingency plan.	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
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-W7, K1-K3	evaluation of student's answers given in the examination form
F2	U1-U3, K1-K3	evaluation of the documentation produced by the examined student
P=40%*F1+60%*F2		

BASIC AND ADDITIONAL READING

1. Krzysztof Liderman, Podręcznik administratora bezpieczeństwa teleinformatycznego, Wydawnictwo MIKOM, ISBN 8372793778
2. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations
3. NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems
4. NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems
5. ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements
6. ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management
7. ISO/IEC 27005 Information technology - Security techniques - Information security risk management
8. RFC 3227, Guidelines for Evidence Collection and Archiving

SUPERVISOR OF COURSE
dr inż. Wojciech Wodo

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Procedury i Bezpieczeństwo Operacyjne
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_W06 K2_W08	C1	Wy1-Wy12	1 2 4 5
W2	K2_W08 K2_W10	C1	Wy1-Wy12	1 2 4 5
W3	K2_W04 K2_W07 K2_W10	C1	Wy1-Wy12	1 2 4 5
W4	K2_W03 K2_W05 K2_W06 K2_W07 K2_W09	C1	Wy1-Wy12	1 2 4 5
W5	K2_W04 K2_W05 K2_W08	C1	Wy1-Wy12	1 2 4 5
W6	K2_W04 K2_W05 K2_W10	C1	Wy1-Wy12	1 2 4 5
W7	K2_W05 K2_W06 K2_W07	C1	Wy1-Wy12	1 2 4 5
U1	K2_U06 K2_U10 K2_U11	C2	Ćw1-Ćw6	3 4 5
U2	K2_U04 K2_U09 K2_U12	C2	Ćw1-Ćw6	3 4 5
U3	K2_U05 K2_U10	C2	Ćw1-Ćw6	3 4 5
K1	K2_K07	C1 C2	Wy1-Wy12 Ćw1-Ćw6	1 2 3 4 5
K2	K2_K04 K2_K08 K2_K09	C1 C2	Wy1-Wy12 Ćw1-Ćw6	1 2 3 4 5
K3	K2_K02 K2_K10	C1 C2	Wy1-Wy12 Ćw1-Ćw6	1 2 3 4 5