SYLLABUS OF A MODULE

Polish name of a module	**Incydenty naruszające bezpieczeństwo**
English name of a module	**Security incidents**
ISCED classification - Code	061
ISCED classification - Field of study	Information and Communication Technologies (ICTs)
Languages of instruction	*English*
Level of qualification: ***1 – BSc (EQF 6)*** ***2 – MSc (EQF 7)*** ***3 – PhD (EQF 8)***	*2*
Number of ECTS credit points	*3*
Examination: ***EO – exam oral*** ***EW – exam written*** ***A - assignment***	*EW*
Available in semester: ***S – Spring only*** ***A – autumn only*** ***Y - booth***	Autumn only

Number of hours per semester:

Lecture	Tutorials	Laboratory	Seminar	E-learning	Project
30		30			

MODULE DESCRIPTION

Module objectives

O1. To familiarize students with the possibilities and techniques of detecting and analyzing threats and responding to security incidents

O2. Students will acquire practical skills in detecting and analyzing threats and responding to security incidents

PRELIMINARY REQUIREMENTS FOR KNOWLEDGE, SKILLS AND OTHER COMPETENCES

1. Knowledge of the functioning of computer networks and network operating systems
2. Ability to use a network protocol analyzer

LEARNING OUTCOMES

LO 1 – The student has knowledge of available tools for detecting and analyzing security threats in IT systems.

LO 2 – The student has the ability to configure operating systems and event recording tools.

LO 3 – The student has competences in the scope of the effects of obtaining network traffic data and recorded events.

MODULE CONTENT

Type of classes – lecture	**Number of hours**
Lec 1 - Information security	**2**
Lec 2 - Operational and human factor safety	**2**
Lec 3 - Physical and environmental security	**2**
Lec 4 - Security incidents	**2**
Lec 5 - Incident detection and characterization	**2**
Lec 6 - Collecting data regarding a security incident	**2**
Lec 7 - Monitoring network traffic and events	**2**
Lec 8 - Analysis of evidence relating to a security incident	**2**
Lec 9 - Introduction to repair techniques	**2**
Lec 10 - Collecting network traffic	**2**
Lec 11 - NSM Operations	**2**
Lec 12 - Server-side security breach	**2**
Lec 13 - Client-side security breach	**2**
Lec 14 - Network and security management systems	**2**
Lec 15 - Pass	**2**
Sum	**30**
Type of classes– laboratory.	**Number of hours**
Lab 1-2 - Introduction to command line and bash	**2**
Lab 3-4 - Defensive security activities - data collection	**2**
Lab 5 - Defensive security activities - data processing	**2**
Lab 6 - Defensive security activities - data collection	**2**
Lab 7 - Real time log monitoring	**2**
Lab 8 - Network monitoring	**2**
Lab 9 - File system monitoring	**4**
Lab 10 -Malware analysis	**2**

Lab 11 - Formatting and reporting results	**2**
Lab 12 - Network and security management systems	**2**
Lab 13 - Security information and event management	**2**
Lab 14 - Responding to computer security incidents	**2**
Lab 15 - Pass	**2**
Sum	**30**

TEACHING TOOLS

1. - lecture using multimedia presentations
2. - preparation of reports on the implementation of the exercises
3. - exercise stands equipped with properly prepared operating systems and software

WAYS OF ASSESSMENT (F – FORMATIVE, S – SUMMATIVE

F1. - assessment of preparation for laboratory exercises
F2. - assessment of the ability to apply the acquired knowledge while doing the exercises
F3. - evaluation of reports on the implementation of exercises covered by the curriculum
F4. - assessment of activity during classes
S1. - assessment of the ability to solve the problems posed and the manner of presentation obtained results - pass mark *
S2. - assessment of mastery of the teaching material being the subject of the lecture - exam

*) in order to receive a credit for the module, the student is obliged to attain a passing grade in all laboratory classes as well as in achievement tests.

STUDENT'S WORKLOAD

L.p.	Forms of activity	Average number of hours required for realization of activity
1.	**Contact hours with teacher**	
1.1	Lectures	30
1.2	Tutorials	
1.3	Laboratory	30
1.4	Seminar	
1.5	Project	
1.6	Consulting teacher during their duty hours	
1.7	Examination	
	Total number of contact hours with teacher:	60

2. **Student's individual work**		
2.1	Preparation for tutorials and tests	
2.2	Preparation for laboratory exercises, writing reports on laboratories	24
2.3	Preparation of project	
2.4	Preparation for final lecture assessment	9
2.5	Preparation for examination	
2.6	Individual study of literature	32
Total number of hours of student's individual work:		65
Overall student's workload:		125
Overall number of ECTS credits for the module		**5** ECTS
Number of ECTS points that student receives in classes requiring teacher's supervision:		2,4 ECTS
Number of **ECTS** credits acquired during practical classes including laboratory exercises and projects:		2,2 ECTS

BASIC AND SUPPLEMENTARY RESOURCE MATERIALS

1. Stallings W., Brown L.: „Computer Security: Principles and Practice (4th Edition)", No Starch Press 2019.
2. Chris Fry, Martin Nystrom, Network Monitoring Security, Helion, 2010.
3. Lee Brotherston, Amanda Berlin, Defensive Safety. Basics and best practices, Helion, 2018
4. Paul Troncone, Carl Albing, Cybersecurity in bash. How to conduct offensive and defensive operations using the command line, Helion, 2021
5. Jason Luttgens, Matthew Pepe, Kevin Mandia, Security Incidents. Response methods in computer forensics, Helion, 2016
6. Richard Bejtlich, Detect and Respond. Practical network monitoring for administrators, Helion, 2014
7. Sabina Szymoniak, Security protocols analysis including various time parameters, Mathematical Biosciences and Engineering, 2021, 18(2): 1136-1153.

MODULE COORDINATOR (NAME, SURNAME, E-MAIL ADDRESS)

PhD Sabina Szymoniak, KI (WIMiI), sabina.szymoniak@icis.pcz.pl