CYBERSECURITY FUNDAMENTALS, MODULE 3 - SYLLABUS

Module code		*Module name*	**Cyberattacks detection and prevention**
Faculty			
Field of study			
Form of study			
Level of study			
Profile			
Status of module			
Person responsible for the module			
Persons teaching the module			

Form of classes	Lectures	Workshops	
Number of hours/sem	6	14	
Semester(s)		ECTS points	
Status		Language of teaching	
Prerequisites	*none*		

Learning objectives
The aim of the course is to acquaint students with the issue of cyber attacks, which may have signs of illegal conduct, as well as with the possible legal qualification of such conduct. The main part of the course is the definition of forms and methods of committing cybercrime (copyright infringement, phishing, malware, ransomware, DoS and DDoS, etc.). An indispensable part of this module is the prevention of these negative phenomena.

Learning outcome	A student who has successfully finished the module will know/be able to/be competent in
KNOWLEDGE	
W1	The student will gain a general overview of national and international legal norms defining illegal activities in cyberspace.
W2	The student will learn the basic technical terminology, which is associated with cyber attacks, cyber incidents, cybercrime, etc. He will be able to distinguish which legal norm, resp. specific provisions apply to a given attack and why.
SKILLS	
U1	After completing the course, the student will be able to identify basic cyber attacks, their modus operandi, caused consequences, etc.
U2	Based on the above identification, the student will be able to apply specific legal institutes of law to the infringement in question. The student will be able to take basic preventive measures aimed at the possible elimination of the negative behavior in the future.
COMPETENCES	
K1	The student is able to distinguish individual cyber attacks, partially controls the legislation relating to protection against these attacks and is able to apply basic preventive measures.

Learning outcomes verification methods									
Learning outcome	Forms of crediting classes								
	Oral exam	Written exam	Partial written task	Final written task (essay etc.)	Test	Project/presentation	Report	Classroom activities	Other…
KNOWLEDGE									
W1		x	x		x			x	
W2		x	x		x			x	
SKILLS									
U1						x		x	
U2						x		x	
COMPETENCES									
K1						x		x	

Criteria for assessing student's competences
The minimal requirements for the three groups of learning outcomes that the Student must obtain in order to pass a given subject are presented below in a synthetic form. In order for the student to pass the module, all learning outcomes described in the syllabus must be positively verified by the person (s) conducting classes within the given module

W - KNOWLEDGE
Rating:
Sufficient - The student remembers and recreates the knowledge to be mastered within the module
Good - The student additionally interprets phenomena / problems and can solve a typical problem
Very good -Student can solve even complex problems in a given field, can make a synthesis, carry out a comprehensive assessment, create a work that is original and inspiring to others.

U - SKILLS
Rating:
Sufficient - The student is familiar with the nature of activities, and is able to perform activities / solve problems related to the content of the module under the guidance of an academic teacher
Good - Student is able to independently perform activities / tasks / solve common problems regarding the content of the module
Very good - The student has a fully mastered ability / ability to perform actions / tasks / problems provided in the content of the module, also in more complex cases.

K - SOCIAL COMPETENCES
Rating:
Sufficient - Student passively absorbs the content of the module, demonstrating the ability to concentrate and listen
Good - The student actively participates in classes, makes assessments that value according to the criteria adopted in a given field, can actively interact within the group
Very good - The student integrates the attitude according to the suggested pattern, develops his own system of professional and social values, is able to assume responsibility for the group's activities, including leadership.

Content of the module (program of lectures and other classes)	Reference to learning outcomes
LECTURES 1. Legal norms regulating cybercrime 2. Social engineering 3. Spam, Scam, Hoax 4. Botnet 5. Cyber attacks - Hacking, cracking, malware, ransomware 6. Cyber attacks - Financially focused attacks of the (phishing	W1, W2 U1, U2, K1

pharming, spear phishing, mobile phishing) 7. Cyber attacks - social attacks (cyberbullying, stalking, sexting, cybergrooming, etc.) WORKSHOPS 1. Analysis of individual cyber attacks and their subsumption under the provisions of the Convention on Cybercrime (ETS No. 185) and national law (Czech Republic, Poland, Portugal) 2. Analysis of individual attacks - modus operandi 3. Security testing against selected attacks. 4. Defining prevention options against individual types of attacks 5. Design of your own solution for protection against individual cyber attacks. 6. Security testing of some systems, applications and data. Students will try to design their own solutions to increase the security of these systems, applications or data. 7. Getting acquainted with tools and resources enabling secure data storage and setting up secure online communication (eg administration and settings of VPN, PGP, password manager, etc.).	

ECTS points balance		
Form of student workload		Number of hours
Number of hours realized with the direct participation of an academic teacher		
1.1	Participation in lectures	6
1.2	Participation in seminars	
1.3	Participation in workshops	14
1.4	Participation in laboratory classes	
1.5	Participation in projects	
1.6	Participation in consultations (2-3 times in a semester)	
1.7	Participation in project consultations	
1.8	Participation in exams/tests	2
1.9	Other…	
1.10	**Number of hours realized with the direct participation of an academic teacher (sum of 1.1 – 1.9)**	22
1.11	**Number of ECTS points obtained by the student during classes requiring direct participation of an academic teacher)**	1,5

Individual work by the student		
2.1	Individual studies (including e-learning lectures)	8
2.2	Individual preparation for workshops	12
2.3	Individual preparation for tests	
2.4	Individual preparation for laboratory classes	
2.5	Preparing reports	
2.6	Implementation of independently performed tasks (projects, documentation)	
2.7	Preparation for the final exam/tests from the workshops	10
2.8	Preparation for the final exam/tests from the lectures	15
2.9	Other	
2.10	**Number of hours of individual work (sum of 2.1 – 2.9)**	45
2.11	**Number of ECTS points obtained by the student during individual study activities**	2,5
Total workload (h)		**67**
ECTS points for the module		**4**

Co-funded by the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.