BASIC INFORMATION:

	Code	*Content*
Organizational unit	01.07.300.	College of Information Technologies
Abbreviation	**FIT-CIT**	
Department	01.06.050.	Department of Computer Communications, Networks and Protection
Subject/module	1.02.01.04.023.	**Cyber threats, attacks and defense technologies**
Broader/additional title		Malware Analysis

TYPE OF SUBJECT:

Functional area	**Specialist**
Level of abstraction	**Advanced**
Type of course-obligation	**Mandatory**

COURSE REGISTER:

	Code	*Content*
Scientific area	1.	Natural sciences
Scientific field	1.02.	Computers and IT
Narrow scientific area	1.02.01.	Computer sciences
Scientific sub-area	1.02.01.04.	Information technologies
Scientific discipline	1.02.01.04.023.	Cyber threats, attacks and defense technologies

COURSE DESCRIPTION:

Educational and professional goals	To identify and understand the threats that jeopardize modern information security systems and to recognize the most common attacks associated with these threats. To use the tools of forensic analysis to identify threats and attacks, to provide technologies for the prevention of attacks, to provide solutions and mitigation, i.e. elimination of consequences.
Competences/educational outcomes	Upon successful completion of this course the student will be able to: • Perform forensic analysis of malware. • Use binary tools for forensic analysis. • Use disassembly tools. • Use debugging tools. • Use sandbox tools to create virtual machine and network environments to isolate suspicious software under controlled conditions and detect its behavior. • Compare static and dynamic analysis of malware. • Illustrate proper laboratory procedures for manipulating malware. • Analyze the sensitivity of a specific malware detector to detect a sample of that software. • Describe possible types of attackers according to specific systems. • Discuss and analyze the limitations of countermeasures for detecting malware based on signature or based on behavioral detection. • Consider how denial of service attacks can be identified and prevented or reduced.

Mastered skills:	Performing malware analysis on computer systems and conducting forensic analysis on local networks, stored data as well as on mobile devices included in corporate platforms. The use of technology to prevent attacks, solve and mitigate or eliminate consequences.
Course content:	Categories of threats (acts of human error, compromise of intellectual property, acts of espionage and unauthorized access, intentional acts of extortion, intentional acts of sabotage and vandalism, theft, intentional software attacks, threats caused by natural forces, deviations of service providers from guaranteed quality, technical errors in the system, errors and deficiencies in the software system, technological obsolescence, errors in management and leadership). Hacking, cracking, digital espionage, hardware and software flaws and errors. Vectors spread and multiply (IP scanning, WEB browsing, computer viruses, unprotected shared resources, mass mail messages, simple and inadequate network protocols). Analysis of individual types of attacks: malicious software (viruses, worms, Trojan horses, spyware, active WEB-scripts), backdoor (back door entry), password cracking (sophisticated methods, brutal force, use of dictionaries), botnets, denial of service overload (Denial of Service DoS), distributed DoS, Mail bombing, IP spoofing (technique of unauthorized access by hijacking TCP packets and implanting one's own content in traffic), Man-in-the-middle, Spam, Sniffers, social engineering social skills), Buffer Overflow, Timing attacks (malicious cookies and retrieving information from Web browsing cache or intercepting cryptographic elements to determine keys and encryption algorithms), Side-channel attacks (side attacks by spying on the screen, electromagnetic radiation, keyboard sound)), adware, SQL injection, cross-site scripting, ransomware, etc. Macro viruses and boot viruses, virus and worm polymorphism. Scams (Virus and Worm Hoaxes) Attacker's goals, abilities and motivation (such as gray economy, digital espionage, cyber warfare, insider threats, hacktivism, advanced threats). Attacks in the field of social engineering (phishing); Tools of forensic analysis, Technologies for prevention of threats and attacks, solving and mitigation, i.e. eliminating the consequences of an attack. About the limitations of malware countermeasures. Unwanted communication through malware, secret channels and steganography. Classes are conducted by elaborating the following topics: Types of threats. Types of malware. Phishing and Spear phishing attacks. DDoS attack. Man-in-the-middle attack. Web application attacks. Advanced Persistent Threat. Ransomware. Attacks focused on user credentials and possible ways of defense. Email vulnerability. Seven phases of implementing advanced threats and possible defense techniques. Cryptographic protection measures. Non-cryptographic protection measures. Basic characteristics of symmetric cryptographic systems. Digital Signature (RSA). Digital Envelope (RSA). User authentication factors. S/MIME protocol. PGP. Desktop security applications. IPSec protocol. Software and hardware protection solutions. Smart card types. Necessary elements for the application of smart cards. HSM devices. Firewall. IAM (Identity and Access Management) system. BCM (Business Continuity Management). NAC (Network Admission Control). Web application firewall. IPS/IDS systems. Web Content filtering. HTTPS inspection. SIEM (Security Information and Event Monitoring). End Point Security System. Secure electronic documentation management. Patch management. Data Loss

	Prevention (DLP).

COURSE METRIC: Regular

ECTS	Teaching activities (classes)					Individual work		TOTAL working hours
	Contact lessons	Exercise trainings	Seminar and stud. papers	Pedagogical workshops	Prof. and clin. practice	Individual and group study	Research	
4	**24**	24				64	8	**120**

COURSE METRIC: Extramural

ECTS	Teaching activities (classes)					Individual work		TOTAL working hours
	Contact lessons	Exercise trainings	Seminar and stud. papers	Pedagogical workshops	Prof. and clin. practice	Individual and group study	Research	
4	**12**	24				76	8	**120**

Lecture languages	**Languages of the people of BiH**			

PREREQUISITES FOR ACCESS

Code	Course/module title	Grade	Description of conditions (additional)
2.09.01.001.	Architecture and organization of computer systems		
2.09.11.011.	Fundamentals of cryptography		
2.09.04.001.	System software (operating systems)		
1.02.02.01.017.	Lower programming languages and program compilers		
1.02.01.02.001.	Network computing		
2.09.10.003.	Protection of computer and business systems		

COURSE METHODOLOGY

During the course, the following activities are envisaged

- ☑ 36 contact hours of interactive lectures;
- ☑ 24 hours for exercises in the field of Cyber threats, attacks and defense technology;
- ☑ 64 hours of individual learning for full-time students;
- ☑ 76 hours of individual learning for extramural students;
- ☑ 8 hours of research.

Lectures according to the established schedule with the use of modern presentation and demonstration tools and techniques with the application of interactive methods of working with students, which provides insight into their prior knowledge and specific experiences based on the issues, but also insight into the continuity of mastering the material. 36 contact hours of interactive teaching are planned for the subject "Cyber threats, attacks and defense technologies".

Lectures are conducted using didactic and educational content in electronic and digital form (which includes recorded lectures and mentoring exercises) on various video presentation media (interactive multimedia optical media).

Application of **information and communication technologies** (ICT) that enable students through Computer Assisted Learning & Research to achieve an active relationship in the process of acquiring knowledge with the help of computer and communication technology, to achieve deeper interaction with teaching content and application of research techniques the very process of acquiring knowledge.

The exercises are intended to acquire practical skills and elaborate practical aspects of various software and hardware technologies for the protection of computer and business systems using technology to prevent attacks, cure and mitigate or eliminate consequences. The content of the exercises is accompanied by thematic units of lectures. During the exercises, the student is obliged to consult with the heads of the competent Department of Computer Communications, Networks and Protection. As specific forms of exercises, **repeaters** are used where assistants/demonstrators prepare students for the exam by offering them a concise overview of the main points of a particular subject. A total of 24 hours of exercise is planned for the subject "Cyber threats, attacks and defense technologies".

Exercises will be performed in the computer room of the Pan-European University or in the Laboratory for Information and Communication Technologies and Distance Learning: (ICT-information & communication technologies & DL-distance learning) or. in university laboratories or in authorized laboratories and/or institutions with which the Pan-European University has concluded agreements on teaching-scientific and business-technical cooperation in which the name and status of the partner institution, teaching base, i.e. university clinical center and university laboratory.

In addition to the planned individual and group learning for the planned duration, it is planned that the student will spend 8 hours researching the source.

STUDENT EVALUATION

No.	Evaluation type	Partial/ Final	Optional/ Mandatory	Perc. of part.
01	Interaction and participation in lectures	Final	Mandatory	15 %
02	Exercise	Final	Mandatory	15%
03	Two colloquiums	Partial	,,	30%
04	Final exam	Final	,,	40%
05				

LITERATURE/RESOURCES (listed in order of importance)

Author (name and surname)	Publication title	Publ. seat	Publisher	Issue year	Type of publ.*
a/ Basic literature					
Charles P. Pfleeger, Shari Lawrence Pfleeger	Analyzing Computer Security: A Threat/Vulnerability/Countermeasure		Pearson Education	2012	coursebook
Michael E. Whitman, Herb Mattord	Principles of Information Security, 4th edition	Boston, USA	Course Technology, Cengage Learning	2012	coursebook
b/ Additional literature					
Prof. Dr.Milan Marković	Lecture materials	Banja Luka	Apeiron	2021	script
Prof. Dr.Milan Marković	Lecture materials	Banja Luka	Apeiron	2021	presentations
c/ Other resources - journals					
Author name and surname *(if the resource is an article)*	Journal title	Publ. seat	Publisher	Issue year	Type of journal
d/ Other resources – WEB					

Website	Webpage	Paper title/hyperlink	Read

(*)Type of publication (coursebook, script, compendium, multimedia)