BASIC INFORMATION:

Organizational unit	01.07.300.	College of Information Technologies
Abbreviation	**FPI-CIT**	
Department	01.06.050.	Department of Computer Communications, Networks and Protection
Subject/module	2.09.10.001.	**Protection of computer and business systems**

TYPE OF SUBJECT:

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

COURSE REGISTER:

Scientific area	**2**	**Technical sciences**
Scientific field	**2.09**	**Computers and IT**
Narrow scientific area	**2.09.10.**	**IT - Information technologies**

COURSE DESCRIPTION:

Educational and professional goals	The aim of the course is for students to acquire basic knowledge in the field of protection of computer and business systems, especially in the environment of application of information technology. The goal of scientific study of this course is theoretical and practical. Students should master the basic concepts in the field of computer and business systems protection. Due to the importance of information as the (most important) resource of the business system, the issue of their security and protection comes to the fore. In order to achieve a high level of security and protection of computer and business systems, comprehensive, complete and diverse protection measures should be applied.
Competences/educational outcomes:	The basic course in Computer and Business Systems Protection presupposes introduction to the concept, subject and goals of computer and business systems protection, regardless of the applied technology, on the one hand, and with the emphasized application of information technology, on the other hand. This course should enable students to acquire the basic knowledge that is the basis for establishing an effective security system for computer and business systems.
Mastered skills:	At the level of computer and business systems security officer
Course content:	The course is realized through the following contents: Digital signature (RSA). Digital envelope (RSA). User authentication factors. Basic components of the S / MIME protocol. PGP. SSL handshake protocol. SSL server and client authentication. IPSec protocol. VPN protocols. Software and hardware protection solutions. Smart card types. Necessary elements for the application of smart cards. HSM devices. Firewall devices. Security of wireless networks in the organization. IAM (Identity and Access Management) system. BCM (Business Continuity Management). NAC (Network Admission Control). SMTP proxy. Web application firewall. IPS / IDS systems. Web Content filtering. HTTPS inspection. SIEM (Security Information and Event Monitoring). End Point Security system. Laptop protection. Incident Response. Manage the lifecycle of user accounts and associated passwords in the

	organization. Combined logical and physical access control and mandatory two-factor authentication of users in the organization. Security Awareness program. Work from a remote location. Secure management of electronic documentation. Patch Management. Privileged Identity Management. Mobile Device Management (MDM). Labeling and classification of data. Database security. Data Loss Prevention (DLP).

COURSE METRIC:

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	
6	**48**	**18**			**20**	**84**	**10**	**180**

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

PREREQUISITES FOR ACCESS

Code	Course/module title	Grade	Description of conditions (additional)
2.09.02.009.	Information system design		
2.09.06.005.	System software (operating systems)		
2.09.03.021.	Databases		
2.09.08.001.	NET management		

COURSE METHODOLOGY

During the course, the following activities are envisaged

- ☑ 48 contact hours of interactive lectures;
- ☑ 18 hours for exercises in the field of protection of computer and business systems;
- ☑ 20 hours of internship;
- ☑ 10 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. **48** contact hours-interactive lessons are planned for the course.

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.

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. 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. **18** contact hours of exercise are planned for the course.

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, ie university clinical center and university laboratory.

Professional/clinical practice is performed inpartner institutions, business organizations, clinical laboratories or authorized independent laboratories for a total of 20 hours. During the exercises, the student is obliged to consult with the heads of the competent Department of Computer Communications, Networks and Protection. For the processing of the subject and professional and clinical practice, it is planned that the student will spend 10 hours on researching the source.

During the internship or exercises, students prepare professional reports that are evaluated by the internship leader. The task of the internship leader and the student within this course is to ensure the mastery and application as a whole, i.e. mastering and applying a number of specific methods and techniques related to the subject.

STUDENT EVALUATION

No.	Evaluation type	Partial/ Final	Optional/ Mandatory	Perc. of part.
01	Exercise	Final	Mandatory	15%
02	Two colloquiums	Partial	„	30%
03	Seminar paper	Final	„	15%
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					
Prof. Dr.Milan Marković	Lecture materials	Banja Luka	Apeiron	2021	script
Džodi R. Vestbi	Međunarodni vodič za borbu protiv kompjuterskog kriminala		Produktivnost AD, Belgrade		coursebook
b/ Additional literature					
Charles P. Pfleger	Security in Computing		Prentice Hall		
B. Schneier	Applied Cryptography		John Wiley & Sons		
S. Castano, M.G. Fugini, G. Martella, P. Samarati,	Database Security		ACM Press		
Pastore M., Dulaney E.	E-Security+		Computer library		
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 – Internet (WEB) resources

Website	Webpage	Paper title/hyperlink	Read

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