BASIC INFORMATION:

Organizational unit	01.07.300.	Faculty of Information Technologies
Abbreviation	**FPI-CIT**	
Chair	01.06.050.	Department of Computer Communications, Networks and Protection
Course/module	2.09.10.015.	**Cyber Law**

COURSE TYPE:

Functional area	**Specialist**
Level of abstraction	**Advanced**
Course type – obligation	**Mandatory**

COURSE REGISTRATION:

Scientific field	**2**	**Engineering Sciences**
Scientific area	**2.09.**	**Computer Science and Informatics**
Narrow scientific field	**2.09.10.**	**IT- Information Technology**

COURSE DESCRIPTION:

Educational and professional goals:	Developing scientific knowledge, academic skills, and practical abilities for the application of legal norms in a digital environment, as well as mastering procedures, methods, and processes for the establishment and protection of rights using modern information technology. The course aims for students to acquire fundamental knowledge in the field of legal aspects of electronic business systems, from the perspective of all subgroups of electronic business (eGovernment, eBanking, eHealth, eCommerce, etc.). The goal of the academic study of this course is both theoretical and practical. Students should gain proficiency in the fundamental concepts of the specific law used within various electronic business systems. Due to the specific nature of electronic business systems in which the parties involved communicate electronically, remotely, and without prior knowledge of each other, it is necessary to adapt the corresponding legal aspects to such business conditions
Competences/educational outcomes:	The foundational course in Cyber Law assumes familiarity with the concept, subject, and objectives of applying legal aspects to electronic business, regardless of the technology applied on one hand, and emphasizes the use of information technology on the other. This course is designed to provide students with essential knowledge that forms the basis for defining relevant legal aspects in various electronic business systems (eGovernment, eBanking, eHealth, eCommerce, etc.). It is expected that the student will: 1) understand the essence and fundamentals of digital technologies, 2) acquire general and specific knowledge about the transformations of law in the digital environment, new manifestations of certain legal institutes, and categories of law in cyberspace, 3) master the process of exercising certain public and private rights before competent authorities, as well as the conclusion of legal transactions in the new environment, 4) be competent in protecting rights using modern information technologies, 5) be able to analytically and critically assess specific concepts and legal solutions in this field in the context of the contemporary digital (information) society.

Skills mastered:	At the level of a Cyber Law Officer
Course content:	Cyber Law is a new area of law that deals with legal issues in the cyber space and encompasses the following: ownership and use of online property - defining the boundaries of ownership in cyberspace and new forms; intellectual property rights - forms, principles, treatment, issues, legal framework (content of rights, methods of protection, rights and obligations of entities); data and their protection (types of data and databases created and used for various purposes; data categories; storage and distribution methods; rights and obligations of entities; attacks and forms of protection; regulation and rule development); personal data, privacy, and privacy infringement, methods of protection, obligations, and responsibilities, European regulations and regulations in the Republic of Srpska and Bosnia and Herzegovina; electronic business in international, national, and self-regulatory activities in creating new frameworks and principles, regulation of competitive behavior, monopolization, and business malpractice; electronic contracts - fulfillment of formalities in formation and execution, evidentiary strength, validity, authenticity, reliability; content, especially illegal and harmful, qualified digital signatures and seals, trust services, European regulations and legal provisions in the Republic of Srpska and Bosnia and Herzegovina; rights and obligations of entities from providers to network operators or system operators and users; cybercrime - forms, execution methods, issues in investigation, tracking, apprehension, and punishment; information security, critical infrastructure, regulation in the Republic of Srpska and Bosnia and Herzegovina, etc. Like any social system, the cyber social system requires global regulation. The 'unlimited' amount of information has made the world global, creating the need for globally harmonized technical and legal frameworks. The aspects of this problem, which are fundamentally important and very complex, are further complicated by the fact that there are a large number of international bodies competent to address this issue. This course, therefore, analyzes the key issues of applying legal aspects in modern computer networks and information systems. It also examines the basic security features of modern computer networks based on Internet technologies and provides an overview of techniques and cryptographic protocols that address these security issues. It discusses trends in network security, potential attacks, possible defense methods, protection technologies, standard cryptographic algorithms, digital signatures, digital envelopes, and multilayer protection architecture. Protection techniques at the application, transport, and network levels of the ISO/OSI model are described, as are trust services based on the use of public key infrastructure. The basic EU legal regulations related to the realization of common legal principles within the European Union related to the aforementioned issues of cyber law (e.g., electronic signatures, privacy protection, electronic documents, e-commerce, electronic invoices/contracts, service directive, etc.) are examined, as well as other applied EU documents (decisions, etc.). Compliance with regulations in the Republic of Srpska and Bosnia and Herzegovina with EU regulations is considered, taking into account specificities. Examples of appropriate legal solutions in environments based on the application of these directives are also discussed, such as: electronic signatures, e-commerce, criminal law, high-tech crime, privacy protection, electronic documents, electronic public procurement, electronic archives, information security, etc.

COURSE METRICS:

ECTS	Teaching activities (hours)						Individual work		TOTAL hours of work
	Contact lessons		Exercises and trainings	Seminar and stud. papers	Pedagogical workshops	Professional and clinical practice	Individual. and group learning	Source research	
	R	V							
4	16	8		24			64	8	**120**

Teaching languages	**Languages of the Peoples in Bosnia and Herzegovina**

ACCESS CONDITIONS

Code	Course/Module title	Grade	Description of conditions (additional)
2.09.02.009.	Information Systems Design		
2.09.06.005.	System Software (Operating Systems)		
2.09.03.021.	Database		
2.09.08.001.	NET management – administration of computer networks		
2.09.08.001.	Computer and Business Systems Security.		

COURSE METHODOLOGY

During the course of the subject, the following are anticipated:

- ☑ 20 contact hours of interactive lectures;
- ☑ 24 hours for student and seminar work in the field of Cyber Law;
- ☑ 8 hours for source research;
- ☑ 64 hours for individual and group learning.

Lectures are conducted according to a set schedule using modern presentation and demonstration tools and techniques, with the application of interactive teaching methods to engage students. This allows for an insight into their prior knowledge and specific experiences related to the discussed topics, as well as monitoring their continuous progress in mastering the subject matter. The subject "Cyber Law" is allocated 20 contact hours of interactive teaching.

Lectures are delivered using didactic and educational content in electronic and digital forms, which include recorded lectures and mentor-led exercises on various video presentation media (interactive multimedia optical media). The teaching, as a whole, is carried out using information and communication technologies (ICT), enabling students to actively engage in the process of knowledge acquisition through computer-assisted learning and research. This facilitates a deeper interaction with teaching materials and the application of research techniques during the knowledge acquisition process.

Practical exercises are designed to acquire practical skills and elaborate on the practical aspects of various software and hardware technologies within the field of Cyber Law. The exercise content corresponds to the thematic units covered in lectures. During exercises, students are required to consult with the coordinators of the Department of Computer Communications, Networks, and Security. Specific forms of exercises, such as tutorials, are used, where teaching assistants and demonstrators prepare students for examinations by providing

a concise overview of key points in a specific subject. Exercises in the "Cyber Law" subject are organized during contact hours as well as within individual and group learning sessions.

Exercises are conducted in the computer lab of the Paneuropean University or in the Laboratory for Information and Communication Technologies and Distance Learning (ICT-information & communication technologies & DL-distance learning), as well as in university laboratories or authorized laboratories and institutions with which the Paneuropean University has agreements on educational, scientific, and business-technical cooperation, resulting in the assignment of the title and status of a partner institution, a teaching base, or a university clinical center and laboratory.

Seminars and student papers are a specific form of independent student work on topics assigned by the nominal professor from the broader program framework of Cyber Law. The goal is for students to comprehensively explore some of the key legal institutes and legal relationships in the field of Cyber Law, cybercrime, intellectual property in cyberspace, privacy and its infringement, e-business, e-contracts, digital signatures, the realization of common legal principles within the European Union related to cyber law issues, electronic documents, electronic public procurement, electronic archives, information security, and the treatment of legal aspects in the areas of eGovernment, eBanking, eHealth, eCommerce, and more.

Through seminars and student papers, students also refine their writing skills and research methods, including the use of academic sources, expanding their knowledge in the thematic area of the seminar paper. Students perfect and defend their work through email correspondence with the relevant professor.

Seminars and student papers must meet methodological criteria for academic writing, standards for proper citation, and requirements for both the "length of the paper" and the "content of the paper" as defined by the mentor or subject professor when assigning the topic, as described in precise instructions provided to the students. The papers must have a length of 3,500 to 4,000 words and include references for all quotes, without direct copying from sources. These papers may be published on the university's website and may be submitted for publication in the annual Proceedings of the Paneuropean University. Each professor may submit for external evaluation and publication no more than 10% of students' seminar or entry papers from one generation of students in the relevant subject.

For the preparation and defense of seminar or other papers in the field of Cyber Law, 24 hours are allocated, along with 8 hours for source research, which is necessary for paper preparation. Papers are submitted electronically, and corrections are made via email exclusively through the university's official email.

Professional/clinical practice will be conducted in partner institutions, business organizations, or authorized independent laboratories. During the practice, students are required to consult with the coordinators of the Department of Computer Communications, Networks, and Security.

While completing their professional practice or exercises, students create professional reports, which are evaluated by the practice supervisor. The goal of the practice supervisor and the student is to ensure that the student comprehensively masters and applies a number of specific methods and techniques related to Cyber Law issues. If a student successfully completes practice in the field of Cyber Law according to the prescribed methodology and submits the required documentation (See: Elective Program of the Faculty of Information Technology), they will earn recognition of this practice in the elective program of the current academic year.

STUDENT WORK EVALUATION

No.	Type of evaluation	partial/ final	elective / mandatory	Percentage of participation
01	Lectures and in-class activities, with electronic access to lectures adjusted by a factor of 0.3 in relation to the number of attended hours.	final	mandatory	15%
02	Seminar Paper	,,	,,	30%
03	Final Exam	,,	,,	55%

LITERATURE / SOURCES (listed in order of relevance)

Author (Last Name, First Name)	Publication title	Publisher's headquarters	Publisher	Edition year	Type of publication*
a/ Basic literature					
Siniša Macan	Sajber pravo i pravni aspekti sajber prostora / Cyber Law and Legal Aspects of Cyberspace.	Banja Luka	Pan-European University Apeiron	2022	Book
Geoffrey Samson,	Law for computing students	UK	eBooks, bookboon.com	2018	Book
b/ Supplementary literature					
Tatiana-Eleni Synodinou Philippe Jougleux Christiana Markou Thalia Prastitou	EU Internet Law in the Digital Era	Cham, Switzerland	Springer Nature Switzerland AG	2020	Book
Rajko Kuzmanović, Siniša Karan	Ustavno pravo / Constitutional Law	Banja Luka	Pan-European University Apeiron	2015	Book
Petar Kunić	Upravno pravo / Administrative Law	Banja Luka	Faculty of Law, University of Banja Luka MoI of the Republika Srpska, Police Education Administration	2010	Book
European Union	Legal regulation related to ICT and the information society				
BIH, EU countries, and neighboring countries	Examples of laws and legal regulations in the field of information and communication technologies, personal data protection, digital identities, and intellectual property				
c/ Other sources – journals					
Author - Surname, First name (if the source is an article)	Journal title	Publisher's headquarters	Publisher	Edition year	Type of journal*

c/ Other sources – Internet (WEB) sources			
Site name	Site address	Title of work/hyperlink	Read
Computers & Security- časopis,	Computers & Security- časopis, Elsevier, USA,	https://www.journals.elsevier.com/computers-and-security	
Portals of Public Institutions in BIH, the EU, and the World			
(*)Type of publication (book, script, compendium, multimedia)			