SYLLABUS OF THE SUBJECT "Informatics and Computer Crimes"

Basic data of the subject	
Academic unit:	Law faculty
Subject title:	Informatics and Computer Crimes
Program:	Law
Level:	Bachelor
Case Status:	Obligatory
Year of studies:	IV/ Semester VIII
Number of hours per week:	3
Credit value – ECTS:	6
Time / location:	Law Faculty
Subject teacher:	**Enver Buçaj Prof.Asoc.Dr**
Contact details:	enverbuqaj@uni-prizren.com
Course description:	The subject "Informatics and Computer Crime", is a scientific discipline that deals with the study of methods that are in function of preventing and combating cybercrime. Cybercrime refers to a wide range of different criminal activities, where computers and information systems are engaged either as a primary tool or as a primary target. Cybercrime includes traditional criminal offenses such as: fraud, forgery and identity theft, offenses related to content e.g. distributing child pornography or inciting racial hatred online, as well as acts that are unique to computers and information systems. e.g. attacks on information systems, denial of service and (malware).
Purpose of the course:	The purpose of this subject can be summarized in the following objectives: - Explain the local and international legal standards that define the policy of preventing and combating cybercrime; - Understanding the institutional and civil mechanisms dealing with the investigation and prosecution of cybercrime; - Identification of the main problems and challenges that this criminal phenomenon presents in a very dynamic current global development.
Learning outcomes:	Upon completion of the course, the student will be able to: - To understand that the dynamic and complex phenomenon of Informatics and cybercrime is one of

	the most current and preoccupying problems for contemporary society; - To form the concept that these forms of manifestation of this phenomenon raises the need for deepening studies on the knowledge of the causes and factors that condition the occurrence of this phenomenon in society; - To know the legal basis for the treatment and prevention of cybercrime through information technology, approaching the analysis of positive legal provisions (de lege lata) and taking into account the need to supplement and change the legal infrastructure in this area (de lege ferenda); - To be equipped with sufficient skills to identify the nature and characteristics of cybercrime in society. All this is done in order for their future jobs to be prepared to react successfully and professionally to this harmful phenomenon for society.

Student workload (should correspond to the student's learning outcomes)			
Aktivitet	**Hour**	**Day/week**	**Total**
Lectures	3	15 javë	45
Theoretical/laboratory exercises	2	15 javë	30
Practical work	2	2	2
Contacts with the teacher/consultations	0.30 min	15	7
Field exercises	0	0	0
Colloquiums, seminars	2	2	2
Homework	2	2	2
Student's independent study time (in the library or at home)	2	15	30
Final exam preparation	2	15	30
Time spent on assessment (tests, quizzes, final exam)	1	1	1
Projects, presentations, etc	1	1	1
Total			**150 hour (6 ECTS)**
Teaching methodology:	During the elaboration and lecture of the problems of Informatics and computer crimes, some methods will be used which are more suitable for providing the		

	material to the students and enabling them to understand the main notions and contents. Thus, the method of active and interactive teaching will be applied, which means exploring and interpreting the fundamental issues of this course by providing students with explanations, data and essential and current information on the phenomena of informatics and computer crimes and their causes. At the same time, this method implies the active involvement of students in debates and treatment of issues that are considered of special interest. Also, the method of studying cybercrime cases through information technology, the methods of interpreting positive legal provisions, the method of analysis of court cases or cases presented in the mass media or reports of governmental or non-governmental organizations on current phenomena of this phenomenon in the world or in the region. In addressing and explaining such problems we will also use other teaching methods and techniques which are more adequate and favorable to the concrete contents. In this way, separate debates will be organized, tests, colloquia, essays and seminars will be applied, which will encourage students to actively and self-initiatedly engage in the teaching process, in learning and advancing the subject matter of this course. As a form of additional engagement, a research project will be prepared with students on the issue of cybercrime through information technology.
Evaluation methodology:	Criteria for the evaluation of students' work and knowledge will be: - Regular attendance of lectures and exercises; - Participation in debates and discussions in class; - Drafting and presenting topics for debates; - Preparation and presentation of seminar papers; - The result of knowledge in colloquia; - The result of knowledge in the exam.
Literature	
Primary literature:	- Enver Buçaj, "Terrorizmi Kompjuterik", Prishtinë, 2015 - Veton G. Vula, "Kriminaliteti Kompjuterik", Prishtinë, 2010 - Copmuter Crime, Investigation, and dhe Law by Chack Easttom and Det. Jeff Taylor;

	- Terrorizmi. Dr. Haki Demolli, 2002; - Kriminalistika. Dr. Vesel Latifi, 2009; - Kriminologjia . Dr. Ragip Halili, 2008; - Kibernetika dhe hyrje ne informatike, Dr. Muhamet Mustafa; - Ligji nr. 03/L-166 për Parandalimin dhe Luftimin e Krimit Kibernetik; - Ligji nr. 04/L-145 për Organet Qeveritare të Shoqërisë së Informacionit; - Ligji nr. 04/L-094 për Shërbimet e Shoqërisë Informatike; - Ligji nr. 04/L-109 për Komunikimet Elektronike; - Ligji nr. 05/L-030 për Përgjimin e Komunikimeve Elektronike; - Ligji nr. 03/L-172 për Mbrojtjen e të Dhënave Personale; - Ligji nr. 04/L-065 për të Drejtën e Autorit dhe të Drejtat e Përafërta; - Ligji nr. 03/L-178 për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë - Kodi nr. 04/L-082 Penal i Republikës së Kosovës; - Kodi nr. 04/L-123 i Procedurës Penale; - Kodi nr. 03/L-193 i Drejtësisë për të Mitur; - Direktiva 2013/40/BE e Parlamentit Evropian dhe e Këshillit, datë 12 gusht 2013, “Për sulmet kundër sistemeve të informacionit”.
Literatura shtesë:	- Kushtetuta e Republikës së Kosovës; - Ligji nr. 03/L-050 për Themelimin e Këshillit të Sigurisë së Kosovës; - Ligji nr. 04/L-076 për Policinë; - Ligji nr. 03/L-142 për Rendin dhe Qetësinë Publike; - Ligji nr. 03/L-063 për Agjencinë e Kosovës për Inteligjencë; - Ligji nr. 04/L-149 për Ekzekutimin e Sanksioneve Penale;

	- Ligji nr. 03/L-183 për Zbatimin e Sanksioneve Ndërkombëtare; - Ligji nr. 04/L-213 për Ndihmën Juridike Ndërkombëtare në Çështje Penale; - Ligji nr. 04/L-052 për Marrëveshjet Ndërkombëtare; - Ligji nr. 04/L-072 për Kontrollin dhe Mbikëqyrjen e Kufirit Shtetëror; - Ligji nr. 04/L-093 për Bankat, Institucionet Mikrofinanciare dhe Institucionet Financiare Jobankare; - Ligji nr. 04/L-064 për Agjencinë e Kosovës për Forenzikë; - Ligji nr. 04/L-198 për Tregtinë e Mallrave Strategjike; - Ligji nr. 04/L –004 për Shërbimet Private të Sigurisë. - Agjencia e të Drejtave Themelore të Bashkimit Evropian, Këshilli i Evropës, Manual i së drejtës evropiane në fushën e mbrojtjes së të dhënave, 2014; - OSCE, Doracak për krimin kompjuterik, 2014.

Designed lesson plan:		
Week	**Lectures**	**Exercise**
First week:	Meaning and subject of "Informatics and cybercrime"	
Second week:	Some aspects of dealing with cybercrime through information technology	
Third week:	Constituent elements of cybercrime and cyber terrorism	
Fourth week:	Legal regulations for cybercrime	
Fifth week:	International acts and prevention of cybercrime; victims and the most common forms of cybercrime victimization	
Sixth week:	Basic forms and characteristics of cybercrime manifestation	
Seventh week:	COLLOQUIUM I Features, dynamics and structure of cybercrime	
Eighth week:	Objective and subjective factors of informatics and cybercrime	
Week nine:	The Balkans and the fight against cybercrime	

Tenth week:	Preventing and combating cybercrime	
Eleventh week:	International cooperation in preventing and combating cybercrime	
Week twelve:	International Aspects of Informatics and Cybercrime	
Thirteenth week:	Computer ethics and education	
Week Fourteen:	Some features on the future of Informatics and Cybercrime Awareness of citizens on the importance of Informatics and the risk of cybercrime, cyber terrorism as a preventive measure	
Fifteenth week:	COLLOQUIUM II	

Academic policies and code of conduct

Students are required to:

- The student must respect the lecture schedule and be attentive in class;
- Adhere to all educational rules;
- The student must be prepared for the lecture by being provided with the relevant book and notebook;
- In respect of their fellow students, they should stop personal telephones during class;
- The student must be an active participant in the lectures;
- The student is obliged to present and possess the ID card in the colloquia and in the final test.

Note

- Participation is a prerequisite for students who want to gain proper knowledge of this course. Students who attend the course regularly will be able to actively participate in the class, giving their concrete contribution during the interactive lectures and during the exercises. Therefore, their contribution to participation and their learning and assignments will be evaluated throughout the semester, in percentage based on pre-defined criteria.