SYLLABUS

Basic information of the course	
University:	**University "Ukshin Hoti" - Prizren**
Academic unit:	**Faculty of Computer Science**
Study program:	**Information Technologies and Telecommunication**
Course:	**Internet security tools**
Study level:	**Bachelor**
Course status:	**Elective**
Study year:	**3**
Number of hours per week:	**2+2**
Credit value - ECTS:	**6**
Time / location:	**It will be published in the university web site!**
Lecturers:	**Assoc. Prof. Dr. Naim Baftiu**
Contact details:	**naim.baftiu@uni-prizren.com**
Course description:	The material is elaborated in order to reinforce and emphasize the basic meanings on the basics of security by giving the basic concepts and illustration of methods for solving security problems on the Internet. In the part of the exercises are given many practical examples that represent a sufficient basis for solving numerical problems where the way of solving the problem and computer security are also discussed.
Course objectives:	Through this course it is possible for students to know the main elements of security and applications for security of sin systems and other enhanced possibilities, which can be offered through synergies of systems and their functionality. - The course analyzes and explains the concepts and principles of security applications. - Internet access relies on the basic concepts and capabilities needed to analyze PC security from potential attacks and actual viruses. - This enables us to understand the types of security as well as security methods as well as many security tools.

	- From this course we understand some logical security methods and cyber-attacks.
Learning outcomes:	After completing this course the students will be able to: - to design and implement basic concepts of Internet security as well as the installation and installation of antiviruses. - The acquired knowledge will be applied in projects and security applications will be made in a concrete way. - Understand the basic concepts of security and cyber-attacks. - Understand the different types of antiviruses and different methods for their installation, etc. - Understand and apply the implementation of various methods for protection against various attacks by viruses and viruses from the Internet.

Contribution on student load (must correspond with learning outcomes)			
Activity	**Hours**	**Days/week**	**Total/hours**
Lectures	2	15	30
Exercise theoretical/laboratory	2	15	30
Practice work	1	2	2
Contact with lecturer/consultations	1	5	5
Field exercises	1	1	1
Midterms	2	2	4
Laboratory exercises	2	2	4
Individual time spent studying (at the library or home)	3	10	30
Final preparation for the exam	5	6	30
Time spent in evaluation (tests, quiz, final exam)	2	3	6
Projects, presentations, etc.	4	2	8
Total			**150**
Notice: 1 ECTS credits = 25 hours commitment, e.g. if the course has 6 ECTS credits student must have 150 hours during the semester.			

Teaching methods:	The course is a combination of lectures, discussions, numerical and laboratory exercises, while the assignments are presented by the laboratory course lecturers!

Assessment methods:	- Attendance in lectures and exercises: 5% + 5%. - Semestral project: 15%. - Midterm 1: 35%. - Midterm 2: 40%. - Or final exam: 100%.	
Assessment and grading:	**Vlerësimi në %**	**Nota përfundimtare**
	91% - 100%	10
	81% - 90%	9
	71% - 80%	8
	61% - 70%	7
	51% - 60%	6
	0% - 50%	5
Literature		
Basic literature:	1. CompTIA Security+, Third Edition, (2011) Wm.A.Conklin, G.White, D. Williams, R. Davis, C. Cothren. 2. Cryptography and Network Security (Principles and Practice) Fifth Edition (2011),W.Stallings. 3. Principles of Computer Security, Second Edition (2011), V.Nestler, Vm.A.Conklin, G.White, M.Hirsch. 4. Standard for the Protection of Information Technol-ogy Equipment CompTIA Security+ All-in-One Exam Guide, Third Edition. Libri "CompTIA Security+". 5. Krahasimet e produkteve Anti-Virus: http://www.av-test.org/en/.	
Additional literature:	1. CompTIASecurity+ All-in-One Exam Guide, Third Edition-1. 2. CompTIASecurity+ All-in-One Exam Guide, Third Edition-2.	
Study plan		
Week	**Lectures**	
First week:	• Introduction to course organization - syllabus (about lectures). • Methods of endangering the security system. • Risk during data transmission	
Second week:	• Types of system risks • Risks from outside. • Risks from within	

Third week:	• Types of viruses • Removal of computer viruses. • Scanning (checking) files. • Tracking Cookies
Fourth week:	• Methods and techniques for securing the system. • Methods of data security (information). • Types of Controls. • Attacks on the server • Modification of server rooms
Fifth week:	• Types and types of malware. • Multiple-Threat Malware. • Blended attack • Firewall
Sixth week:	• Wireless security techniques • Internet networks and security. • View from WLAN-Internet network • Free flight area of WLAN networks
Seventh week:	• Secret actions of viruses in commercial services
Eighth week:	• Test 1
Ninth week:	• Software protection on PC. • Special units of viruses
Tenth week:	• Border control at the entrance and exit of the PC. • Memory and ranking strategy
Eleventh week:	• Physical equipment for controlling access to the computer.
Twelfth week:	• Computer hardware security • Application security. • Types of hardware and software security firewalls.
Thirteenth week:	• Computer passwords • Password protection • IP Security (IPsec). Two security protocols
Fourteenth week:	• Authentication technology • The security components of an Information System. • Security procedures
Fifteenth week:	• Test 2

Exercises

Study plan	
Java	**Exercises**
First week:	• Introduction to course organization – syllabus (about exercises).

	• The laboratory shows how viruses attach, how they multiply and what they contain.
Second week:	• Authors of viruses, • their functioning and their elimination. • Students work in groups in the laboratory to eliminate viruses.
Third week:	• What is the web and its security? • Take a concrete case of a company's web and start with its security, starting from the database to their publication
Fourth week:	• Case study of computer networks and their security. • Works in a group of students for the opening and security of networks in the laboratory.
Fifth week:	• Case study of external risks • Case study of risks from within • Checking the system and identifying the Trojan horse and Worms virus.
Sixth week:	• In the laboratory is done how to remove viruses of different types. • What are the types of antivirus for PC installation? • A concrete case is taken for the installation of anti-virus and its installation from the PC.
Seventh week:	• Analysis of the defense and operation of a practical server during the attack.
Eighth week:	• Consultations about the colloquium 1.
Ninth week:	• Changes in the actions of anti-virus types. • A comparison of two types or even more types of antivirus is presented.
Tenth week:	• Types of wired and wireless networks and their security. • In a practical way, the types of networks are presented in the laboratory, their security is presented by means of a licensed antivirus.
Eleventh week:	• Hardware parts and their physical safety • Prevention of infections in the application software
Twelfth week:	• Changing the IP number. • Encryption and decryption algorithms
Thirteenth week:	• Internet security and sending E-mails – Secrets • cryptography practical matter concrete examples
Fourteenth week:	• Verification technology - concrete case study in the laboratory

Fifteenth week:	• Consultation about midterm 2.

Academic policies and rules of conduct
• Generally lecture presentations will be made through MS PowerPoint, tables, material usage, computer programs and numeric exercises. • Additional resources (scientific papers, publications, national bulletins, as well as recent discoveries and research) will be provided by professors. • In the absence of the opportunity for practical work to be organized weekly, in cooperation with the management of the university, this activity will be organized on certain days in: organizations, companies, etc. • During each session will be organized the conversation and co-participation with the students! • Students are required to be regular in lectures and exercises! • It will be evaluated when the students collaborate and participate in the lectures and course exercises! • Timely arrival in lectures and exercises is mandatory!