SYLLABUS

1. Data about the program of study

1.1	Institution	The Technical University of Cluj-Napoca
1.2	Faculty	Electronics, Telecommunications and Information Technology
1.3	Department	Communications
1.4	Field of study	Electronics and Telecommunications Engineering
1.5	Cycle of study	Master of Science
1.6	Program of study/Qualification	Multimedia Technologies/ Telecommunications/ Master
1.7	Form of education	Full time
1.8	Subject code	TM-E16.20/ TC-E01.00

2. Data about the subject

2.1	Subject name	Security in Telecommunications Networks									
2.2	Subject area	Electronics and Telecommunications Engineering									
2.3	Course responsible/lecturer	Associate Professor Daniel ZINCA, PhD									
2.4	Teachers in charge of applications	Associate Professor Daniel ZINCA, PhD									
2.5	Year of study	II	2.6	Semester	3	2.7	Assessment	Exam	2.8	Subject category	DS/DO

3. Estimated total time

Year/ Sem.	Subject name	No. of weeks	Course [hours/ week]	Applications [hours/ week]			Course [hours/ semester]	Applications [hours/ semester]			Indiv. study	TOTAL	Credits
				S	L	P		S	L	P			
I/1	Advanced Design in Computer Networks	14	1		2		14		28		58	100	4

3.1	Number of hours per week	4	3.2	of which, course	2	3.3	applications	2
3.4	Total hours in the curriculum	56	3.5	of which, course	28	3.6	applications	28

Individual study	Hours
Manual, lecture material and notes, bibliography	20
Supplementary study in the library, online and in the field	10
Preparation for seminars/laboratory works, homework, reports, portfolios, essays	18
Tutoring	3
Exams and tests	3
Other activities	

3.7	Total hours of individual study	58
3.8	Total hours per semester	100
3.9	Number of credit points	4

4. Pre-requisites (where appropriate)

4.1	Curriculum	N.A
4.2	Competence	Network security. Firewall. IDS/IPS, CBAC, IPSec site-to-site VPN, IPSec and SSL remote access VPN, AAA. WLAN Security. Switch security

5. Requirements (where appropriate)

5.1	For the course	Cluj-Napoca
5.2	For the applications	Cluj-Napoca

6. Specific competences

Professional competences	CP 3 - Installation, configuration, operation and maintenance of hardware and software for complex telecommunications networks. CP 7 - Evaluation of performance, service quality and security of telecommunications systems
Cross competences	CT 3 - Ability to understand technical requirements and propose solutions

7. Discipline objectives (as results from the key competences gained)

7.1	General objectives	Developing the competences regarding the use, configuration, design of network security devices.
7.2	Specific objectives	1. Recognizing and understanding basic concepts specific to network security. 2. Developing skills and abilities necessary for the configuration of network security devices. 3. Developing skills and abilities for the design of network security installation.

8. Contents

8.1. Lecture (syllabus)		Teaching methods	Notes
1	Course description. Basic concept. Network security	Presentation, heuristic conversation, exemplification, problem presentation, teaching exercise, case study, formative evaluation	Use of .ppt presentation, projector, blackboard
2	Security policies. Security architectures		
3	Network Security devices. Device hardening.		
4	Firewalls. Host-based firewalls. Network-based firewalls. Zone-based firewalls.		
5	AAA Authentication, Authorization, Accounting. The RADIUS protocol The TACACS+ protocol.		
6	Intrusion Detection Systems IDS. Intrusion Prevention Systems IPS.		
7	Data Link layer security for LANs. Switch features		
8	WLAN Wireless LAN security. Standards, threats, solutions for Cisco devices		
9	VPNs Virtual Private Networks. Standards. IPSec protocol architecture		
10	IPSec Site-to-site VPNs		
11	IPSec Remote-Access VPNs. SSL VPNs		
12	Cisco ASA security devices. Features. Firewall implementation		
13	Introduction to Cyber Security		
14	Recapitulation. Preparation for the final exam.		
8.2. Applications (lab)		Teaching methods	Notes

1	Introduction. Presentation of the networking devices to be used (Cisco 1812W, 2911 family). Labour protection	Didactic and experimental proof, didactic exercise, team work	Use of laboratory instrumentation, experimental boards, computers, magnetic board
2	Usage of Cisco Configuration Professional CCP for selecting the basic security features of Cisco IOS devices		
3	Cisco IOS Firewall configuration. CBAC, ip inspect. Zone-based firewall.		
4	AAA configuration of Cisco IOS devices using RADIUS protocol. Installation and configuration of a RADIUS server.		
5	IDS configuration. Snort rules configuration and application		
6	LAN security. VLAN security. Configuration using Cisco Catalyst 2960 switches.		
7	WLAN security configuration on Cisco 1812W and Cisco Aironet AP		
8	Site-to-site VPN using Cisco IOS devices. Preshared keys and digital certificates		
9	Remote-access VPN using Cisco IOS devices. The Easy VPN server and Easy VPN remote components.		
10	SSL VPNs. WebVPN feature of Cisco IOS devices		
11	Cisco ASA devices. Firewall configuration		
12	Introduction to cyber security		
13	Laboratory test		
14	Lab recovery and finalization of laboratory activity		

Bibliography

1. D. Zinca, Computer Networks (in Romanian). Editura Risoprint, Cluj-Napoca 2006
2. A.S. Tanenbaum, D.J. Wetherall, *Computer Networks. Fifth Edition*, Prentice Hall 2010
3. Cisco Press – CCNA Security Official Exam Certification Guide, 2018
4. Cisco Press – CCNA Cyber Operations Official Exam Certification Guide, 2018

On-line references

5. Cisco Networking Academy, https://www.netacad.com

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

Competences acquired will be used in the following COR occupations (Electronics Engineer; Telecommunications Engineer; Electronics Design Engineer; System and Computer Design Engineer; Communications Design Engineer) or in the new occupations proposed to be included in COR (Sale Support Engineer; Multimedia Applications Developer; Network Engineer; Communications Systems Test Engineer; Project Manager; Traffic Engineer; Communications Systems Consultant).

10. Evaluations

Activity type	10.1	Assessment criteria	10.2	Assessment methods	10.3	Weight in the final grade
Course		The level of acquired theoretical knowledge and practical skills		Theoretical Test (mark T) : 18 questions		- T, max 10 pts. 50%
Applications		The level of acquired abilities		Project (P): oral and practical exam based on laboratory and project work		- L, max. 10 pts. 50%
10.4 Minimum standard of performance						
$N=(T+P)/2$, $N \geq 5$, $T \geq 5$, $P \geq 5$						

Date of filling in	Course responsible	Teachers in charge of applications
01.07.2020	Associate Professor Daniel ZINCA, PhD	Associate Professor Daniel ZINCA, PhD

Date of approval in the department	Head of Communications Department
01.10.2020	Professor Virgil DOBROTA, PhD