Syllabus

1. Program information

1.1. Institution	ACADEMY OF ECONOMIC STUDIES
1.2. Faculty	Economic Cybernetics, Statistics and Informatics
1.3. Departments	(Departament) INFORMATICA SI CIBERNETICA ECONOMICA
1.4. Field of study	Economic Informatics
1.5. Cycle studies	Master Studies
1.6. Education type	Full-time
1.7. Study program	IT&C Security
1.8. Language study	English
1.9. Academic year	2016-2017

2. Course information

2.1. Name	**Computer Network Security**								
2.2. Code	**16.0241IF1.2-0001**								
2.3. Year of studies	**1**	2.4. Semester	**2**	2.5. Assessment type	**Exam**	2.6. Course type	**O**	2.7. Number of ECTS	**4**
2.8. Instructors									

3. Total estimated time

3.1. Number of weeks	14.00		
3.2. Number of hours per week	2.00	of which	
		C(C)	1.00
		S(S)	1.00
3.3. Total hours from curriculum	28.00	of which	
		C(C)	14.00
		S(S)	14.00
3.4. Total hours of study per semester (ECTS*25)	100.00		
3.5. Total hours of individual study	72.00		
Time distribution for individual study			
Study the textbook, course support, bibliography and notes			
Further reading in the library, on the online platforms and field			
Preparing seminars, labs, homework, portfolios and essays			
Tutoring			
Examinations			
Other activities			

4. Prerequisites

4.1. About curriculum	Cryptography Basis, Security Standards and Protocols
4.2. About skills	The course assumes no prior compenteces.

5. Requirements

C(C)	Course lectures take place in rooms with multimedia teaching equipment.
S(S)	Laboratories are held in rooms that have PCs with Internet access. The development environment used is Microsoft Visual Studio 2010 or 2012, Ubuntu within virtual machines with GCC, Java plus necessary tools.

6. Skills covered

	C2	Using modern computer technology for risk management in life cycle stages of software systems
	C4	Scientific research and designing of IT security solutions for the entire range and complexity of software architectures

7. Course objectives

7.1. General objective	Presentation of security mechanisms and services at different architectural levels of the computer networks. Gathering knowledge concerning network security management: security policies development, security auditing. Assuring security for router devices, for web servers and VPN.
7.2. Specific objectives	Transfer tehnologic pentru asimilarea cunostintelor pentru: -IPSec -HTTPs -VPN -S/MIME -configurare IDS, IPS si firewall

8. Course contents

8.1. C(C)		Teaching methods	Advices
1	INTEGRITY OF THE SECURITY WITHIN NETWORK ARCHITECTURES Informatic vulnerabilities, cryptography's role, network and security architecture, services and mechanisms for network security		
2	IDENTIFICATION AND AUTHENTICATION MECHANISMS FOR NETWORKS Identification methods, biometric methods, authentication and non-repudiation protocols		
3	IP LEVEL SECURITY; VPN NETWORKS Ipsec protocol, Private Virtual Networks Architectures		
4	TRANSPORT LAYER SECURITY - SSL secure protocols, TLS secure protocols		
5	ELECTRONIC MAIL SECURITY PEM standard (Privacy Enhanced Mail), MOSS standard (MIME Object Security Services), S/MIME standard, security in X.4000 standard, PGP program (Pretty Good Privacy)		
6	FIREWALL SYSTEMS - Components of a firewall, Firewall architectures examples, Implementing security using firewalls		
7	TECHNICAL COMPONENTS OF SOME OF THE SECURITY POLICIES Access control, Network security through the user's eyes, Network security through the administrator's eyes, Securing web servers and Internet applications, Securing the network by using firewall and VPN mechanisms, Developing security policies for an organization, Auditing methods for network security.		

Bibliography

- Patriciu V., Bica I., Pietrosanu M, Vaduva C, Voicu N., Securitatea comertului electronic, All, 2001
- Patriciu V., Pietrosanu M., Bica I., Cristea C., Securitatea informatică în UNIX şi INTERNET, Tehnica, 1998
- Patriciu V., Criptografia si securitatea retelelor de calculatoare, Tehnica, 1994
- Stalling Willliam, Cryptography and Network Security, Prentice Hall, 1999

8.2. S(S)		Teaching methods	Advices
1	INTEGRITY OF THE SECURITY WITHIN NETWORK ARCHITECTURES Informatic vulnerabilities, cryptography's role, network and security architecture, services and mechanisms for network security		
2	IDENTIFICATION AND AUTHENTICATION MECHANISMS FOR NETWORKS Identification methods, biometric methods, authentication and non-repudiation protocols		
3	IP LEVEL SECURITY; VPN NETWORKS Ipsec protocol, Private Virtual Networks Architectures		
4	TRANSPORT LAYER SECURITY - SSL secure protocols, TLS secure protocols		
5	ELECTRONIC MAIL SECURITY PEM standard (Privacy Enhanced Mail), MOSS standard (MIME Object Security Services), S/MIME standard, security in X.4000 standard, PGP program (Pretty Good Privacy)		
6	FIREWALL SYSTEMS - Components of a firewall, Firewall architectures examples, Implementing security using firewalls		
7	TECHNICAL COMPONENTS OF SOME OF THE SECURITY POLICIES Access control, Network security through the user's eyes, Network security through the administrator's eyes, Securing web servers and Internet applications, Securing the network by using firewall and VPN mechanisms, Developing security policies for an organization, Auditing methods for network security.		

Bibliography

- Patriciu V., Bica I., Pietrosanu M, Vaduva C, Voicu N., Securitatea comertului electronic, All, 2001
- Patriciu V., Pietrosanu M., Bica I., Cristea C., Securitatea informatică în UNIX şi INTERNET, Tehnica, 1998
- Patriciu V., Criptografia si securitatea retelelor de calculatoare, Tehnica, 1994

9. Course contents corroboration with the demands of epistemic community representatives, professional associations and representative employers

Taking into account the best practices from IT&C field applied by big companies such as: Intel, Oracle, Microsoft, IBM, HP and professional consortiums such as: Apache, Red Hat, ISO/IEC.

10. Assessment

Activity	Assessment criteria	Assessment methods	Percentage in the final grade
10.1. S(S)		Applied activities, practical or project certificates/laboratory/tests, tests during the module, auditing tests	40.00
10.2. Final assessment		Final examination	60.00
10.3. Grading scale	Whole notes 1-10		
10.4. Minimum performance standard	Knowledge required: configuration of security protocols IPSec and HTTPs. The point granted by default is included in the weights assigned to the types of assessments.		

Completion date,
07/10/2016

Instructors,

Approval date of department

Director of department,