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	**Antivirus and Virus Technologies**								
2.2. Code	**16.0241IF1.1-0004**								
2.3. Year of studies	**1**	2.4. Semester	**1**	2.5. Assessment type	**Exam**	2.6. Course type	**O**	2.7. Number of ECTS	**5**
2.8. Instructors									

3. Total estimated time

3.1. Number of weeks	14.00		
3.2. Number of hours per week	3.00	of which	
		C(C)	2.00
		S(S)	1.00
3.3. Total hours from curriculum	42.00	of which	
		C(C)	28.00
		S(S)	14.00
3.4. Total hours of study per semester (ECTS*25)	125.00		
3.5. Total hours of individual study	83.00		
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	Object Oriented Programming, Secure Applications Programming
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

	C3	Using modern computer technologies for developing components that ensure maximum IT security
	CT1	Applying the rules and values of professional ethics for decision making and independent or team implementation of complex tasks / objectives at work

7. Course objectives

7.1. General objective	Presentation, analysis and implementation of the protection mechanisms, technologies and techniques against virus and hacker software attacks, using the assembly language.
7.2. Specific objectives	Transfer tehnologic pentru asimilarea urmatoarelor: -ASM x86 -crearea virusilor paraziti si companion -crearea modulelor antivirus de stergere virusi si detectie

8. Course contents

8.1. C(C)		Teaching methods	Advices
1	1. Programming techniques in ASM and C/C++ for creating viruses and antiviruses.		
2	2. Creating COM viruses – overwriting, companion and parasitic in ASM 8086.		
3	3. Creating EXE viruses in ASM x86.		
4	4. Creating memory resident viruses in ASM x86.		
5	5. Creating boot viruses in ASM x86.		
6	6. Creating source code viruses in C/C++.		
7	7. Macro-viruses: Office – Word, Excel, E-mail.		
8	8. Antiviruses design principles.		
9	9. Boot viruses detection and boot antivirus creation in ASM x86.		
10	10. File system viruses detection and antivirus creation in ASM x86 and C/C++.		
11	11. Memory resident viruses detection and antivirus creation for memory resident viruses in ASM x86.		
12	12. Anti-hacker methods and techniques; Thinking the architecture of a secure system for prevention against virus, logical bombs and trojan horses attacks.		
13	13. Sniffer applications: definition and fundamentals; useing the sniffer applications.		
14	14. Anti-virus development sample		

Bibliography

- Mark Ludwig, The Little Black Book of Computer Viruses, American Eagle Publication Inc, 1995
- Mark Ludwig, The Giant Black Book of Computer Viruses, American Eagle Publication Inc, 1997
- Ion Ivan, Cristian Toma , Informatics Security Handbook - 2nd Edition, ASE Publishing HouseASE Publishing House, 2009

8.2. S(S)		Teaching methods	Advices
1	1. Programming techniques in ASM and C/C++ for creating viruses and antiviruses.		
2	2. Creating COM viruses – overwriting, companion and parasitic in ASM 8086.		
3	3. Creating EXE viruses in ASM x86.		
4	4. Creating memory resident viruses in ASM x86.		
5	5. Creating boot viruses in ASM x86.		
6	6. Creating source code viruses in C/C++.		
7	7. Macro-viruses: Office – Word, Excel, E-mail.		
8	8. Antiviruses design principles.		
9	9. Boot viruses detection and boot antivirus creation in ASM x86.		
10	10. File system viruses detection and antivirus creation in ASM x86 and C/C++.		
11	11. Memory resident viruses detection and antivirus creation for memory resident viruses in ASM x86.		
12	12. Anti-hacker methods and techniques; Thinking the architecture of a secure system for prevention against virus, logical bombs and trojan horses attacks.		
13	13. Sniffer applications: definition and fundamentals; useing the sniffer applications.		
14	14. Anti-virus development sample		

Bibliography

- Mark Ludwig, The Little Black Book of Computer Viruses, American Eagle Publication Inc, 1995
- Mark Ludwig, The Giant Black Book of Computer Viruses, American Eagle Publication Inc, 1997
- Ion Ivan, Cristian Toma , Informatics Security Handbook - 2nd Edition, ASE Publishing HouseASE Publishing House, 2009

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)			40.00
10.2. Final assessment			60.00
10.3. Grading scale	Whole notes 1-10		
10.4. Minimum performance standard	Knowledge required: building in ASM x86 of a parasitic virus and a anti-virus module. 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,