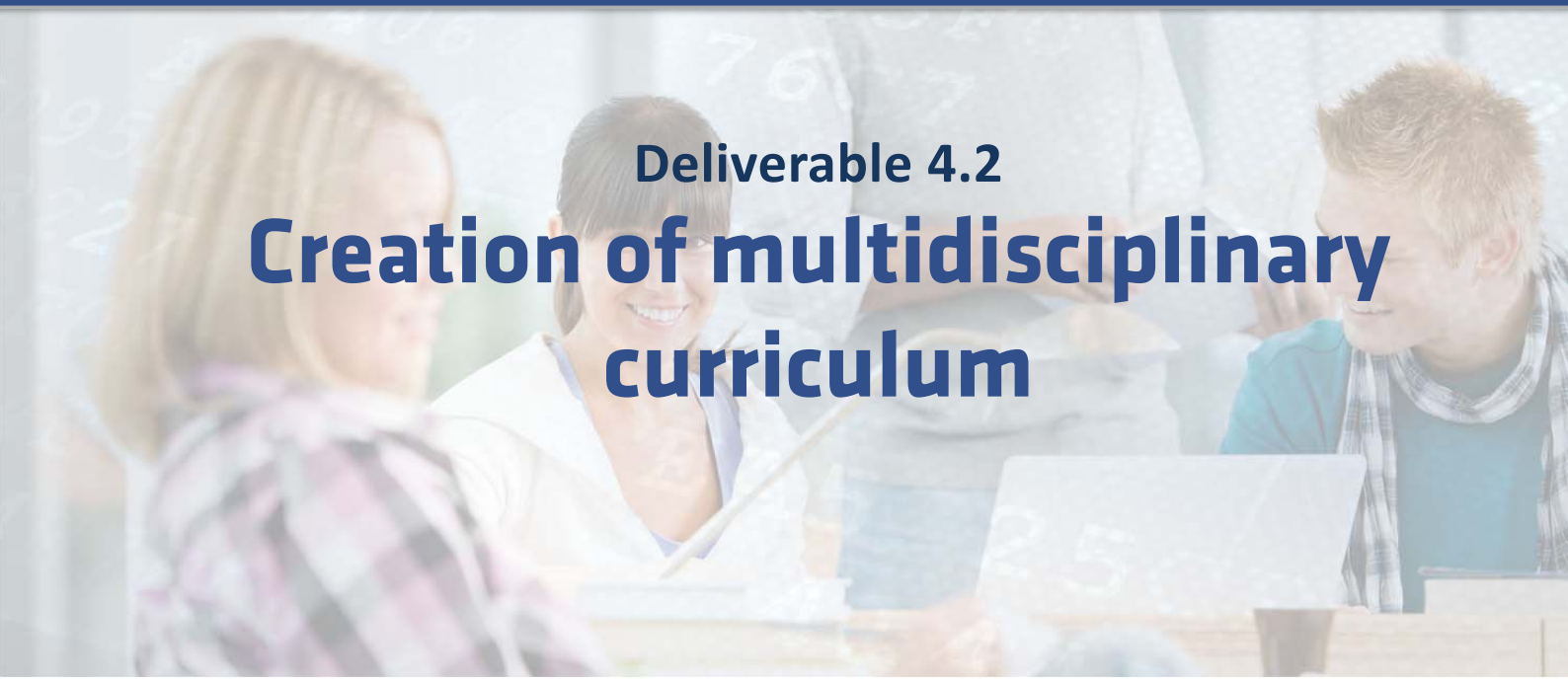

Deliverable 4.2

Creation of multidisciplinary curriculum

Tempus

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

Deliverable 4.2

Creation of multidisciplinary curriculum

European Commission Tempus Project:

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of content

1. Introduction

The threats to ICT systems are evolving all the time and to mitigate the threats requires professional actions at all levels, in companies, institutions and state level. The need for the new professionals in the field of cyber security is constant and the programs in the universities should be developed to meet the needs. The universities in Montenegro have started developing courses and projects and initiated projects to support the activities as soon as they understood the need for master level education in cyber security.

The development of the first version of the programme started in parallel to the evaluation of ECESM project and was accredited before the project started in one of the partners of the project University Donja Gorica. The new version of the programme was developed during the project. The specific needs where identified, analysed, and discussed during the project. Also the experience of the partners and best practices in other universities were taken into account in developing a new version of the program. It turned out that it is possible and reasonable to modify the existing program without reaccreditation. The initial program was focused on cyber security management. It was identified that the needs are broader and the new program was developed with 3 specializations:

1. Cyber security technology
2. Cyber security policy and economy
3. Cyber security management

As the laws of Montenegro do not allow joint programs, it was decided that in addition to the crucial enhancements in the cyber security study programme of University Donja Gorica, a cyber security module is developed inside the Information Technology program in Mediterranean University. This consists of new cyber security courses and allows IT students to specialise to cyber security. Enhanced services and facilities at Montenegrin Cyber Educational Centre will be used by both partner universities for education and training activities. A modern well-equipped laboratory of network and mobile security and forensics has been developed in the centre during the project as an important contribution to the highlevel cyber security education in Montenegro.

The best practices of the cyber of the existing cyber security master programs in Europe and in the world was analysed as the basis of the program development. One of the important conclusions was that although the field of cyber security is interdisciplinary and very wide, it is important to also the technical specialists in addition to management and overall politics level security administration. The main effort went to developing a technical specialization of the program and also the additional equipment was bought to support the technical cyber security courses in the partner universities in Montenegro.

In the following the developed study program and courses are described. Also the summary of suggestions are that given for further development of the program in the future.

2. Background

In this section we put similar explanations as those submitted to EACEA in July 2016. The Letter requested approval for changes in Master study program at UDG, new courses at study program at University Mediterranean, as well as purchase of new specialised equipment for these programs.

Project proposal planned to establish new Master study program in cyber security, but during evaluation phase, due to identified importance of the study program, partner organisation University Donja Gorica has already accredited it. Existing Master study programme at University Donja Gorica is highly specialized in the field of cyber security management, while modern cyber society needs specialists in different fields of specializations, including technical aspects, policy and economy, management. Thus, existing Master study programme at University Donja Gorica must be improved with courses recognized by EU universities in the three specializations:

1. Cyber security technology
2. Cyber security policy and economy
3. Cyber security management

Table 1 shows existing Master study programme, while its improvement is presented in Table 2.

Table 1.Existing Master study programme in UDG

Course	**ECTS**	**SEMESTER**
Introduction to Management of cyber security	6	1
National and international security	6	1
Cyber Crime	6	1
Introduction to Cryptography	6	1
Methodology of Scientific work	6	1
Law and ethical aspect of cyber security	6	2
Modern Cyber security issues and technologies	6	2
Master Thesis	6	2
TOTAL	**60**	

Innovated program will be implemented at the University Donja Gorica, while the University Mediterranean will update existing Master study programme in Information Technology with courses in the field of cyber security technology, thus enabling specialization in the field of cyber security for their students.

Proposed innovations are expected to result with:

- Improved education and training approaches implemented at ME HEIs in the field of cyber security (since Master study programme is highly focused on ICT aspects of cyber security, high quality teaching and learning process will impose equipped laboratories with appropriate software and hardware components, as well as modern literature).
- More specialized professionals in different fields of cyber security in ME.
- New opportunity for young researchers in cyber security to specialise their focus areas (compared to one more general existing approach).
- Enhanced services established at Montenegrin Cyber Educational Centre in ME (Newly equipped laboratory will be used for both, education and training processes at both partner universities, the University Donja Gorica and the University Mediterranean.

ECESM Quality Assurance Board agreed that proposed approach is the most efficient solution which addresses the needs for education of cyber security professionals in Montenegro, in respect to variety factors, such as: the size of Montenegrin population, the number of HEIs, expected number of students, as well as valid legislation in Higher Education System in Montenegro.

ECESM Quality Assurance Board also agreed on the necessity for adequate equipment for the purpose of: critical infrastructure protection, digital forensics, network and software security, etc. (which was not initially planned by project application).

3. Updated Master study program and courses

Cyber security program in University Donja Gorica

The cyber security master program in University Donja Gorica is going to have a major upgrade to be able to educate professionals in several directions in the cyber security field.

The goal of the program is to give broad knowledge and practical skills in cyber security. Students can specialise to technology, policy or management tracks. A graduate of the program specializing in cybersecurity is ready to be employed as a technical professional or a manager in the field of cyber security.

The program is a 1-year program that is common to Montenegro 4+1 higher education system. The suggestions for upgrading the program to 2-year program is described later in the document.

The curriculum consists of a common compulsory part and three specialization modules consisting of elective courses. The overall structure of the study program is presented in Table 1. It consists of 2 compulsory courses on both semester, elective specialization block in the first semester and writing the thesis on the second semester.

To make the broad study program with different specializations feasible in the country of size of Montenegro only one specialisation is opened for every admission. The new programme is applied and new courses given to the students admitted to the programs in 2016.

EU partners of the project have contribute to the development and teaching of the courses.

Course	**ECTS**	**SEMESTER**
National and international security	6	1
Cyber Crime	6	1
Elective courses for specialization	18	1
Management of Cyber Security	6	2
Methodology of Writing a Scientific Paper in Academic Settings	6	2
Master Thesis	18	2
TOTAL	**60**	

Table 1: Cyber security curriculum

CYBER SECURITY TECHNOLOGY		
Course	**ECTS**	**SEMESTER**
Security Architectures and Network Defense	6	1
Introduction to cryptography	6	1
Modern Cyber security issues and technologies	6	1
Digital forensics	6	1
TOTAL	**24**	

Table 2: Technology specialisation

CYBER SECURITY POLICY AND ECONOMY		
Course	**ECTS**	**SEMESTER**
Cyber terrorism, theory and practice	6	1
Enterprise Cyber security	6	1
Legal and Ethical Aspects of Cyber security	6	1
Legal and Regulatory Aspects of Electronic Commerce	6	1
TOTAL	**24**	

Table 3: Policy and Economy specialisation

CYBER SECURITY MANAGEMENT		
Course	**ECTS**	**SEMESTER**
Modern Cyber security issues and technologies	6	1
Enterprise Cyber security	6	1

Information Risk Management and Governance	6	1
Industrial Espionage and Counterfeiting	6	1
TOTAL	**24**	

Table 4: Management specialisation

Cyber security program in Mediterranean University

It was found during the analysis that there is no need to develop a second independent cyber security master study program in country of size of Montenegro. The current law do not allow to have a joint program also. It was found that the best solution is to update the existing Information Technology program instead. A module of cyber security courses will be added to the program, so that the students with strong IT background can specialise to cyber security. They can improve their knowledge and skills in general cyber security topics, and the security of information systems and mobile software and also to the basic forensics in the wearable IT devices present everywhere. The list of the courses is presented in Table 5.

Course	**ECTS**
Cybercrime and Cyber Security	6
Advanced Systems of Information System Security	6
Digital forensics of Mobile Phones	6
TOTAL	**18**

Table 5: Cyber security courses in UNIM

4. Upgrading to 2-year program

Having in mind announced changes in high education system in Montenegro, which will include, among the others: 3+2 system, which means that graduate studies will last 3 years, and then Master studies 2 years; as well as upcoming reaccreditation of University of Donja Gorica (at 2017 year), it is proposed to create 2-year program for Cyber security specialisations.

Recommendation: Create and make accreditation of 2-year program in all 3 Cyber security specialisations. The 1st year shall include more general courses providing basics about Computer Networks, Cyber Security

5. Conclusions

The new study programme is developed in one Montenegrin partner university and a module of cyber security courses in another partner university. Also a joint centre is founded and modern laboratories equipped in the centre to support the courses. The

resulting programs and courses form a strong basis for raising a new generation of cyber security professionals in Montenegro.

Appendixes

A. Course syllabi of cyber security program of UDG

Course name	***National and International Security***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	n/a
Objectives	The aim of this course is to provide students with the knowledge of fundamental concepts of the security such as the roots, theories, institutions, operational frameworks as well as to offer the students the comparative analysis of the national security systems of the individual countries so that they become aware of the fact that the security is one of the basic prerequisites for the development of an individual, state and international community in general.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Theories of international security – Realism, • Liberalism, Marxism, Post-modernism, so on, • Modern institutionalisation of international security- a cooperative approach (UN, EU, OSCE, and so on), • Theory of conflict prevention in International • Relations, Globalization and security (the change of view on security after the Cold War, the influence of globalization on international politics / relations), • Contemporary security challenges in International Relations (humanitarian intervention as a warning measure in 21st century), • National security – concept, system, significance, and challenges), • Components of national security system: defence system of a modern state, the system of internal affairs, and protection and relief system, • Analytical framework of national security system of the South-Eastern countries in Europe

Learning outcomes	At the end of the course, the student should be able to: demonstrate a fundamental knowledge of issues related to war, peace and security within contemporary national and international society; use relevant theoretical frameworks to analyse issues of war, peace and security in different parts of the world, and demonstrate understanding of the key concepts in national and international security. The acquired knowledge will become a solid basis for further development of the student's competences and skills, for the analysis of security practice by deploying policies and strategies of security, as well as for further research of the impact of cyber security on national and global security as a whole.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. Bailys, John (ed.) 2008. The globalization of world politics: an introduction to international relations. Oxford, New York: Oxford University Press. 2. Booth, Ken. 2007. Theory of world security. Cambridge: Cambridge University Press. 3. Cvrtila V., Tatalović, S., Grizold A., Suvremene sigurnosne politike, Golden marketing, Zagreb, 2008. 4. Grizold, A., Međunarodna sigurnost: teorijsko institucionalni okvir, Fakultet političkih znanosti, Zagreb, 1998. 5. Cvrtila, V., Države i međunarodna sigurnost, Politička misao. vol XXXIV broj 3/1997. 6. Lovrić D., Upravljanje krizama i strategija nacionalne sigurnosti SAD-a, Međunarodne studije, Vol. I, broj 4/2001
Other remarks	

Course name	***Cyber Security Management***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	This module emphasises the need for good security management. Its aims are to identify the problems associated with security management and to show how various (major) organisations solve these problems.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	There will be 11 sessions lasting about three hours. Most sessions will consist of a lecture given by an outside industrialist, including the opportunity for questions and answers on the topics discussed. Students are also expected to engage in appropriate private study and to take part in the online discussion forums. The list of topics may vary slightly to reflect developments in the subject but examples of recently covered topics are: • Security: What, Why, How? • The Principles of Information Security and its Management • Internal Control, Audit and Security • Information Security, Governance and the Law • IS 27001 – Information Security Management for Business Benefit • The Role of Risk Analysis and Management in Effective Information Security. • Security Management – Systems, Models and Frameworks • Building a World-class Information Security Architecture • The Business of Trust • Information Security Management in the Real World • Business Continuity – the Wider Context of Information Security
Learning outcomes	On completion of the module, the student will be able to evaluate security management requirements; critically analyse alternative security management strategies and methods; propose effective methods for solving security management problems, and compare and critically evaluate different approaches to security management.

Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. Steve Purser, A Practical Guide to Managing Information Security, Artech House, 2004 (Library location: 001.6425PUR). 2. Gurpreet Dhillon, Principles of Information System Security: text and cases, Wiley, 2007 (Library location: 001.6425DHI). 3. Editors: Krause and Tipton, Handbook of Information Security Management, CRC Press, 2001. 4. Scott Barman, Writing Information Security Policies, New Riders, 2002. 5. Seymour Bosworth and M.E. Kabay (Eds), Computer Security Handbook, Fourth Edition, Wiley, 2002. 6. Harry B. DeMaio, B2B and Beyond, Wiley, 2001. 7. Gurpreet Dhillon, Managing Information Systems Security, MacMillan, 1997. 8. Donn B. Parker, Fighting Computer Crime, Wiley, 1998.
Other remarks	

Course name	***Introduction to Cryptography***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	The approach of this module is non-technical. The primary objectives are to explain why cryptography is needed, what it provides, how basic cryptographic mechanisms work and what issues need to be addressed when implementing cryptography. The mathematical content of this module is minimal. Tutorial support for the elementary mathematics needed for this part of the course will be provided for those who require it.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	This course is divided into three parts: • Setting the Scene: the need for cryptography; core security services provided by cryptography; basic model of a cryptosystem; historical cryptosystems; security in theory and practice • The Cryptographic Toolkit: symmetric encryption algorithms; hash functions; message authentication codes; entity authentication techniques; pseudorandom number generators; public key encryption algorithms; digital signatures; freshness techniques; cryptographic protocols • Cryptography in Practice: key management; public key infrastructures; legal aspects of cryptography; cryptographic applications
Learning outcomes	At the end of this module, students should be able to: explain exactly what cryptography can be used for; appreciate the differences between various types of cryptosystems and in which situations they are most usefully employed; identify the issues that need to be addressed when assesing what types of crypotgraphic mechanism are necessary to "secure" an application; describe several basic cryptographic mechanisms for providing each of the core security services; identify the limitations of cryptography and how to support it within a full security architecture. Students completing this module should not expect to be able

	to design algorithms.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. F. Piper and S. Murphy, Cryptography: A Very Short Introduction, Oxford University Press, 2002. 2. A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
Other remarks	

Course name	*Cyber crime*
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	The aim of the module is to provide students with a solid foundation to understand the concepts involved in and the characteristics of cyber security and cybercrime. Its aims are to understand Computer Crime, together with its social and legal implications; understand the techniques and mechanisms for cyber security attacks and frauds; and understand how to use appropriate counter measures.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Types of computer crime, origins, overview, statistics, and global relations. • Legal measures: Computer abuse, damages induced by a criminal activity, software piracy, fraud and falsification, investigative authority. • Case studies: hacking investigations, hacking cases, computer misuse. • Projecting and victim selection and procurement • Spamming, phishing and pharming • Malware: types, effects and investigation • DoS and distributed DoS: Causes, mechanisms, case studies and counter-measures. • Network crime: Methodology of Internet hacking and hacking of other networks • Investigations, incident processing, and forensic assessment • Future: Internet expansion, dissemination of pornography and other obscene material, • Identity theft and fraud
Learning outcomes	Upon the successful completion of this course, students should be able to: • Identify and evaluate tendencies in computer crime • Associate methodologies of computer security with investigative methods and techniques • Discover criminal activities in computer settings. • Apply criminal and civil laws on computer crime • Explain how malware and other techniques of technical

	hacking are used by the criminals • Understand mechanisms used by hackers of how they made the scheme and selected their victims. • Assess the mechanisms deployed for launching DoS and distributed DoS attacks and apply the appropriate counter-measures. • Compare and evaluate the attitudes and responses of the businesses, governments and media to the cases of computer crime.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. D.E. Denning, Information Warfare and Security, Addison-Wesley, 1999 2. Hedly & Aplin, Blackstone's Statues on IT and E-Commerce, Oxford University Press 3. E. Casey, Digital Evidence and Computer Crime, Academic Press, 3rd Edition, 2011 4. E. Wilding, Information Risk and Security: Preventing and Investigating Workplace Computer Crime, Gower, 2006.
Other remarks	

Course name	***Methodology of Writing a Scientific Paper in Academic Settings***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	The aim of the course is to introduce the students to the logical structure of science, fundamental scientific notions, help them formulate scientific hypothesis, make the students acquainted with the scientific hypotheses, laws and theories, familiarize the students with the subject matter, methodology, mission and significance of science. The course introduces the language of research, ethical principles and challenges, and the elements of the research process within quantitative, qualitative, and mixed methods approaches. Students will use these theoretical underpinnings to begin to critically review literature relevant to their field or interests and determine how research findings are useful in informing their understanding of their environment (work, social, local, global).
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Paradigm, theory and research • Causality in social sciences and humanities and researches • Structuring the research • Conceptualisation, operationalisation and measurement • Indexes, scales and typologies • Sample, importance, models and typology • Stages of conducting a survey • Quantitative data analysis • Fundamental statistical methods for data analysis • Qualitative research • Interview, method, importance, data gathering and processing • Evolutional research • Power, politics and ethical issues
Learning outcomes	Upon the completion of the course, the participant will be able to: • Understand research terminology

	• Be aware of the ethical principles of research, ethical challenges and approval processes • Describe quantitative, qualitative and mixed methods approaches to research • Identify the components of a literature review process • Critically analyze published research
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. Đ. Šušnjić, Metodologija, Beograd, 1999. 2. D. Marsh, S. Gerry, Theory and Methods in Political Science, Basingstoke: Palgrave, Macmillan, 2003. 3. R. Hague, M. Harrop, Comparative Government and Politics, London: Palgrave, 2001
Other remarks	

Course name	***Modern Cyber Security Challenges & Technologies***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	This course will: provide an overview of the fundamental technologies underpinning computer and networked applications, along with the associated security issues; examine how maintaining security through separation is a key aspect of operating system design; provide an overview of the main types of authentication mechanisms used in computer systems; describe the fundamental types of access control mechanisms; overview the fundamental principles of secure protocol design, and how they are used in deployed security protocols; examine the security threats and vulnerabilities found in particular types of networks; assess mobile and wireless communication technologies in terms of their security vulnerabilities.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Introduction to Computer and Network Architectures • Introduction to Security • Platform and Operating System Security • User Authentication Mechanisms • Security Models and Access Control Mechanisms • Malicious Code • Introduction to Security Protocols • Network Security Threats and Countermeasures • Web Security • Wireless (WLAN and GSM/UMTS) Security
Learning outcomes	On successful completion of the course students will be able to: demonstrate a systematic understanding of the construction of information networks, specifically the architecture and operation of the Internet Protocol suite; demonstrate a clear understanding of the construction of a modern computer system, specifically the different hardware and software components which support multiprocessing; explain the causes and potential effects of vulnerabilities that affect computer systems and identify appropri-ate countermeasures; demonstrate a comprehensive

	understanding of different types of user authentication mechanisms in use within modern computer systems; provide an overview of different access control mechanisms used within computer systems, and evaluate the suitability of different access control mechanisms for different security requirements; provide a clear understanding of how strong authentication protocols, key exchange protocols and key exchange mechanisms suitable for use on open networks can be constructed; demonstrate a clear understanding of how the design principles for secure protocols are applied to the Internet, focusing on SSL / TLS; identify the key security threats faced in network environments, and be able to specify appropriate countermeasures; explain the basic differences between different wireless technologies, and evaluate the security requirements according to the particular needs of different wireless networking technologies.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. D. Gollmann, Computer Security (2nd Edition), John Wiley & Sons, 2005. 2. C.P. Pfleeger and S.L. Pfleeger, Security in Computing (3rd Edition), Prentice-Hall, 2002. 3. W. Stallings, Network Security Essentials (3rd Edition), Prentice-Hall, 2007.
Other remarks	

Course name	*Digital Forensics*
ECTS	6
Lectures (hours)	20
Labs (hours)	20
Seminars (hours)	20
Individual work (hours)	60
Prerequisites	
Objectives	The module provides a fast-paced overview of the field of digital forensics, covering approaches and techniques for gathering and analysing traces of human and computer-generated activity in such a way that it is suitable for presentation in a court of law. Beginning with legal and procedural aspects, the module encompasses live as well as conventional storage and network forensics with particular emphasis on the limitations and possible counter-forensics techniques employed by skilled adversaries. The module aims to help gain an appreciation of underlying first principles of ways in which data that can subsequently be used as evidence is generated, stored, and transmitted in different environments and mechanisms for both collection and analysis.
Teaching and learning methods	Labs, lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	The course will cover the following main topics: • Introduction to Digital Forensics • Windows Host Forensics Fundamentals • Unix and Linux Host Forensics Fundamentals • Network Forensics • Malware • Special Devices and Systems • Steganographic Mechanisms and Covert Channels • Alternative Storage Mechanisms
Learning outcomes	On completion of the module, students will have gained an understanding of key legal and procedural aspects of digital evidence and procedures required to safeguard these for use in a court of law. They will also have a well-grounded understanding of the loci in host operating systems and network components where human or computer-generated activity will produce traces which can be identified and analysed as well as the uncertainties associated with collecting such information. Particular emphasis will have been placed on ways in which

	such evidence may be contaminated or its acquisition obfuscated or disabled altogether by malicious software or counter-forensics mechanisms.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. K. J. Jones, R. Beitlich, C. W. Rose, Real Digital Forensics: Computer Security and Incident Response, Addison-Wesley, 2006 2. M. Russinovich, D. Solomon, Windows Internals, 5th ed. Microsoft Press, 2009 3. B. Carrier:, File System Forensic Analysis, Addison- Wesley, 2005 4. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2nd ed. Morgan Kaufmann, 2007 5. D. P. Bovet, M. Cesati, Understanding the Linux Kernel, 3rd ed. O'Reilly, 2005 6. C. Benvenuti, Understanding Linux Network Internals, O'Reilly, 2005 7. D. Liu, Cisco Router and Switch Forensics, Syngress, 2009 8. R. McDougall, J. Mauro, Solaris Internals, 2nd ed. Prentice-Hall, 2006 9. J. Zdziarski, iPhone Forensics, O'Reilly, 2008 10. C. H. Malin, E. Casey, J. M. Aquilina, Malware Forensics: Investigating and Analyzing Malicious Code, Syngress, 2008 11. T. Cohen, A. Schroader, Alternate Data Storage Forensics, Syngress, 2007 12. E. Casey, Digital Evidence and Computer Crime, 2nd ed. Academic Press, 2004
Other remarks	

Course name	***Legal and Ethical Aspects of Cyber security***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	The cyber security of physical or information systems is not a stand-alone concern. There exists a set of ethical principles set down internationally, in terms of fundamental rights (e.g. privacy and protection of personal data), which applies to the cyber domain, just as it applies to the physical domain. Legislation has also been put in place which sets out rules for the protection of these ethical principles in the context of cyber security. In addition, the increasing demand for more open and interconnected cyber systems raises new ethical and legal issues in the protection of the these systems and, particularly, the information which they handle. This module will examine the ethics of cyber security technologies and relevant current laws, in terms of the often competing priorities of governments, corporations and the citizens.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Introduction to legal aspects of Internet use • Responsibilities for the activities carried out in cyberspace • Electronic commerce and contract law • Dematerialization of IDs, Legal restrictions on the movement and use of cryptographic technologies. Digital signature and Law on Electronic signature. • International electronic commerce, electronic money and legislature on how they should be used • Introduction to cyber ethics: concepts, perspective and methodology • Critical thinking skills and logical argumentation skills. • Tools for cyber ethics practice improvement • Privacy in the cyberspace • Professional ethics, code of conduct and moral responsibility • Jeopardising the intellectual property in cyberspace • Digital gap and work transformation • Community, personal identity and self-awareness in

	cyberspace • Ethical aspects of development and application of technologies
Learning outcomes	Upon the successful completion of the course, the student will: • Be aware of the legal aspects of Internet use • Understand where lies the responsibility of use and operating in cyber environment • Become familiar with the ways of operating of electronic commerce, its types and risks which it can carry. • Acquaint themselves with the legislature necessary for the establishment of e-commerce and required infrastructure needed for its effectuation. • Be familiar with the legal restrictions concerning the use of cryptographic technologies • Be informed about fundamental concepts, perspectives and methodologies which define the ethical behaviour in cyber space • Understand the notion of privacy and adopt the code of conduct and moral responsibility in cyber space • Understand the ways of how they can jeopardise the private property right and how they can transform its operations in cyber space • Be familiar with ethical aspects of development and application of modern technologies.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. C. Reed, Internet Law: Text and Materials, Butterworths, 2004. 2. H. Tavani, Etics and Technology, ontroversies, Questions, and Strategies for Ethical Computing, John Willey and Sons, 2011
Other remarks	

Course name	***Security architectures and Network Defence***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	This module defines the cyber security context and introduces a broad range of cyber security terminology in order for students to comprehend future study concerning the cyber domain. Security architectures to segregate differing trust domains via security devices, especially stateful packet filtering firewalls, are introduced and analysed, together with the mindset that any particular defence will fail at some point, necessitating layered defence in depth. The complexities of managing the relationship between the desired network security posture and the true network security posture is examined from the perspectives of testing, monitoring and audit. The overall aim of the module is for students to comprehend the common security controls available to prevent, detect and recover from network security incidents and to mitigate risk.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Firewalls • Advanced Filtering • Firewall Configuration • Hardening: Establishing a Secure Baseline • Intrusion Detection and Prevention • Protecting Web Applications • Memory Analysis • Endpoint protection • Securing Wireless
Learning outcomes	The module aims: • to develop a broad understanding of the key techniques and technologies used to defend information-communication networks from attack; • to explain the enterprise context within which network defence functions, and the roles, processes, and impact upon the wider enterprise activities that network defence can have;

	• to develop the ability of candidates to understand not only what is involved in network defence, but also how it contributes to an overall information and network risk-management strategy; • and to provide an economic context within which investments in network defence can be judged.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. S. Convery, "Network Security Architectures", Pearson Higher Education ©2004, ISBN:158705115X 2. J. Zheng, A. Jamalipour, "Wireless Sensor Networks: A Networking Perspective" 3. T. Alpcan, T. Başar, "Network Security: A Decision and Game-Theoretic Approach"
Other remarks	

Course name	***Cyber terrorism, theory and practice***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	This subject explores the reasons why terrorists utilise the online environment along with an analysis of the costs and benefits they accrue in doing so. It develops a holistic, critical, and wide-ranging understanding of current and future implications related to the use of cyberspace by terrorists. The counter terrorism measures deployed against such use of cyberspace will also be covered. Students will critically engage with both primary (through secure subscription services) and secondary resources related to terrorist use of cyberspace, and analyse and critique counter efforts undertaken by both government and the private sector in combatting such use of cyberspace.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Terrorism as Communication • Wars of Ideas: Information Operations, Psychological Operations • Propaganda, Recruitment, Facilitation • Critical Infrastructure and 'Cyber Terrorism' • The Evolution of Terrorism in Cyberspace • Social Media and Terrorism • Case Study: ISIS and Social Media • 'Going Dark' - Terrorism and Encrypted Platform • Counter Measures: Intelligence, Law Enforcement • Counter Measures: Private Sector • Over the Digital Horizon: The Future of Terrorism in Cyberspace
Learning outcomes	Upon successful completion of this subject, students should: • be able to demonstrate advanced knowledge of terrorists' use of cyberspace and related counter terrorism contexts, including understanding of historical, contemporary, and ongoing developments in terrorist use of cyberspace • be able to demonstrate a knowledge of research principles and methods applicable to terrorism and cyberspace • be able to demonstrate the application of these research

	principles and methods to the intersection of terrorism and cyberspace issues at an operational, strategic, and policy level • be able to reflect critically on theory, professional practice and scholarship in relation to terrorism and cyberspace • be able to analyse and evaluate critically complex ideas and concepts related to terrorist use of cyberspace, and apply those ideas and concepts in diverse contexts • be to demonstrate technical research and communication skills to justify and interpret theoretical propositions, methodologies, conclusions and professional decisions to specialist and non-specialist audiences
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. "Cyber terrorism: Understanding, Assessment, and Response", Editors: Chen, Tom, Jarvis, Lee, Macdonald, Stuart (Eds.), Springer-Verlag New York, 2014 2. "Cyber Warfare and Cyber Terrorism", L. Janczewski, A. Colarik, 2007 3. "UNDERSTANDING CYBERCRIME: P H E N O M E N A , C H A L L E N G E S AND LEGAL RESPONSE", ITU, 2012
Other remarks	

Course name	***Enterprise Cyber security***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	Comprehensive framework for managing all aspects of an enterprise cyber security program. It enables an enterprise to architect, design, implement, and operate a coherent cyber security program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Introduction: Enterprise security and risk analysis. • Identity management • Access control • Web service security. Enterprise web service security and SAML. REST security and OAuth • Enterprise security patterns. • Operating Enterprise Cyber security • Security and privacy in the cloud.
Learning outcomes	• persuasively articulate cyber security imperatives to key decision makers in an organisation. • critically evaluate the cyber security posture of an organisation. • critically analyse “identity” in the context of the cyber security of an organisation's mission, considering both those inside and those outside the organisation. • critically analyse the cyber security consequences of the increasing connectedness of end-point devices and control systems (such as sensors, actuators, buildings and transportation) to an organisation's mission.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C

	• 80-89 B • 90-100 A
Literature	1. Ross Anderson, Security Engineering, 2nd ed., Wiley, 2008. ISBN 0470068523 2. Deepak Alur, Dan Malks, and John Crupi, Core J2EE Patterns: Best Practices and Design 3. Enterprise Cybersecurity 4. Donaldson, S., Siegel, S., Williams, C.K., Aslam, A., How to Build a Successful Cyberdefense Program Against Advanced Threats, 2015
Other remarks	

Course name	***Legal and Regulatory aspects of Electronic Commerce***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	Defending intellectual property, navigating privacy concerns, and negotiating contracts. Key legal issues related to conducting business electronically. Complying with the regulatory environment governing cyberspace, and the technological trends and developments affecting e-commerce.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Domain Name Protection in E-Commerce • The More Things Change, the More They Stay the Same: Legal Issues in Technology Contracts • Intellectual Property Issues in E-Commerce • Overview of Significant Legal Trends and Issues for E-Commerce • Regulations and Legislation in Cyberspace • Responding to claims of online slander or defamation • Taxing eCommerce
Learning outcomes	• Describe the key technological elements comprising electronic commerce systems • Examine the legal nature of communications • Explain the evidential problems of computer-derived evidence • Be able to briefly outline issues in consumer protection law and how they apply to eCommerce. • Explain how self-regulation mechanisms can operate. · • Identify different forms of consumer ADR · • Be able to define the term "spam", discuss the problems is causes and identify some technical and legal measures to prevent spam • Understand the different issues of concern to rights-holders and users • Be able to explain how jurisdictional issues can be problematic • Be able to explain the benefits and drawbacks of some of the

	alternative methods of internet content control · • Be able to analyse the need for, and scope of, content-related regulations in a national context • ·Be able to understand the importance of Information Security to eCommerce • Be able to identify different categories of personal data in a commercial transaction • Be able to recognise the difference between residence and source based taxation · • Detail the problems which e-commerce poses to international tax rules
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. D. M. Ruscitti, H.J. Hammond, B. Lockwood, R. Raysman, "Understanding the Legal Aspects of E-Commerce: Leading Lawyers on Defending Intellectual Property, Navigating Privacy Concerns, and Negotiating Contracts(Inside the Minds)", 2011 2. "Handbook on Electronic Commerce", edited by Michael Shaw, Robert Blanning, Troy Strader, Andrew Whinston, Springer 2012 3. A. Ath. Gkoutzinis, "Internet Banking and the Law in Europe: Regulation, Financial Integration and electronic commerce", 2006
Other remarks	

Course name	***Information risk management and governance***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	The course covers the principles of applied information security management and is suitable for those who are looking for an in-depth understanding of security management in medium to large organisations. The course comprises the following topics: governance and security policy, threat and vulnerability management, incident management, risk management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations. Under these broad headings, the following areas covered: ISO 27000 series and the Plan-Do-Check-Act model, assessment of threats and vulnerabilities, incident response, forensics and investigations, risk assessment and risk management frameworks, dealing with classified/ sensitive data, contingency planning, legal and regulatory drivers and issues, certification, common criteria, securiy awareness, education and training, and practical considerations when implementing the frameworks to address current and future threats.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Characteristics of Risks in the Modern World • Risk Perspectives • Risk Governance: An Overview • Pre-assessment and Framing of Risk • Risk Characterization and Evaluation • Risk Management • Risk Communication • Stakeholder and Public Involvement • Organizational Security Models (COSO, ITIL, COBIT 4.X, ISO 27000 Series, etc.) • ISO 27001
Learning outcomes	The successful participant will: • have an understanding of the key themes and principles of information security management and be able to apply these principles in designing solutions to

	managing security risks effectively; • understand how to apply the principles of information security management in a variety of contexts; • have an appreciation of the interrelationship between the various elements of information security management and its role in protecting organisations.
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	1. Aven, Terje, Renn, Ortwin, "Risk Management and Governance: Concepts, Guidelines and Applications", Springer-Verlag Berlin Heidelberg, 2010 2. By Alexander Borek, Ajith Kumar Parlikad, Jela Webb, Philip Woodall, "Total Information Risk Management: Maximizing the Value of Data and Information Assets", 2013 3. ISO/IEC 27001 - Information security management
Other remarks	

Course name	***Industrial espionage and counterfeiting***
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	This course examines the motivations for industrial espionage and the various method of attack on the physical security of an organisation, its electronic infrastructures and its staff and suppliers. Student will learn to analyse and mitigate potential attacks through industrial espionage; will develop an understanding of counterfeiting attacks and design countermeasures; and will carry out risk management processes in both industrial espionage and counterfeiting
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Industrial Espionage: Motives and Threats of Industrial Espionage Defined • Espionage Tradecraft • Cyber Espionage • Developing a Counterespionage Program • Protecting Proprietary Classified Information • Physical Security • The Human Resources Department and Counterespionage • Counterespionage Resources
Learning outcomes	• analyse exposure to industrial espionage. • synthesise appropriate mitigation to industrial espionage exposure. • critically analyse exposure in products and services to counterfeiting • synthesise appropriate countermeasures to counterfeiting exposure in products and services
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D

	• 70-79 C • 80-89 B • 90-100 A
Literature	1. Daniel J. Benny, "Industrial Espionage: Developing a Counterespionage Program", CRC Press , 2013 2. I.I. Androulidakis, F.E. Kioupakis, "Industrial Espionage and Technical Surveillance Counter Measurers", Springer International Publishing, 2016
Other remarks	

B. Course syllabi of cyber security courses in UNIM

Course name	***Advanced System of Information System Security***
Course description (1 sentence)	Through this course students acquire basic knowledge about computer systems security and protection
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	60
Prerequisites	
Objectives	Acquiring knowledge in the field of Information systems security. Students will be presented possible security methods, as well as potential risks for threatening IS.
Teaching and learning methods	Lectures, seminars, seminar papers, mid-term exams, and final exam.
Course content (topics covered)	• Theory security databases and software • The most common security risks of databases and software, practical examples • Ways of identifying potential security risks in data bases and software, searching for known vulnerabilities and establishing new ones. • Network security principles. • Safe operating systems on the network. • Network intrusion detection, intrusion prevention, methods and use of tools. • Applied Cryptography. Modern techniques of data encryption and decryption by using cryptographic algorithms Block encryption and block encryption methods, hash functions and message authentication codes. • Problems of protection of information resources in a company. Tools and techniques for assessing IS security in organizations. • IS security principles and models, and security management in large systems • Security procedures implementation issues> technical, legal and physical. • Good practice and experience IS security related analysis of socio-political and ethical issues. • Creating the best safety procedures based on technical needs and in accordance with the consciousness of people who are to carry out a given procedure. • Security systems in accordance with the law.

	• Risks of identity theft and prevention methods, risks of phishing and protection against phishing
Learning outcomes	-
Students responsibilities	Students have to attend lectures and seminars. They shall regularly do homework, two mid-term exams, and final exam
Assessment	- Homework 5 points - Regular attendance 5 points - Mid-term exam I 20 points - Mid-term exam II 20 points - Final exam 50 points A student has to pass both mid-term exams (over 50%) and gains a passing grade on the final exam
Literature	D. Gibson „CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide“,2014. W. Stallings„Cryptography and Network Security. Principles and Practice “,Prentice Hall, fifth edition 2011. Scripts from lectures and seminars
Other remarks	n/a

Course name	*Cybercrime and Cyber Security*
Course description (1 sentence)	• International legal framework against cyber crime. International cooperation. • Review of the Convention on Cybercrime (CETS No.195) and legislation in EU member states that treats this problem. Protocol to the Convention on cyber crime which refers to the incrimination of acts of a racist and xenophobic nature committed through computer systems. • Legislative and legal framework in Montenegro and the results of its implementation. • Examples of good practice in tackling cybercrime • • Ways of organizing in the fight against cybercrime
ECTS	6
Lectures (hours)	30
Labs (hours)	0
Seminars (hours)	30
Individual work (hours)	85
Prerequisites	
Objectives	The objective of this course is that students learn the basic principles and requirements imposed by the fight against cybercrime. Cybercrime or high technology crime, with currently known forms of its appearance, is a global problem for developed countries, as well as for medium developed and developing countries. Today there is no aspect of organized criminal activity which in one form or stage of its realization does not use cyber space, such as drug trafficking, money laundering, organized crime and corruption, arms smuggling, financial fraud, child pornography and others. Students will be introduced to possible ways of organizing in the fight against cybercrime, as well as the review of the organizing in the EU and Montenegro. Students will be introduced to the tools used in the fight against cybercrime and the tools used for advanced digital forensics.
Teaching and learning methods	Lectures, seminars
Course content (topics covered)	• Cyber security strategy High-tech crime (HTC), cybercrime, computer crime • Types of HTC HTC – examples from practice • Trends in the development of responses to illegal activities • Formulating response strategies

	• Denial of service attacks EU directives related to network security Information security • The establishment of an organizational infrastructure for information security • Computer systems in service of cybercrime International standards and suggestions • Critical information infrastructure security
Learning outcomes	
Students responsibilities	Students have to attend lectures and seminars. They shall do project assignments, mid-term exams and final exam.
Assessment	The exam consists of mid-term exams I and II, seminar paper and final exam which may be written or oral. In order to pass the exam, a student has to gain minimum 51% points on mid-term exams I and II and on final exam and project assignment. The final grade is formed after summarizing the points for pre-exam and exam assignments. - Mid-term exam I - 20 points - Project work I revision – 5 points - Mid-term exam II - 20 points - Project work I revision – 5 points - Final exam consists of oral presentation and demonstration of final project information system - 50 points In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	Džodi R.Vestbi, '' Međunarodni vodič za borbu protiv kompjuterskog kriminala '' ISBN 86-901301-3-6. Američka advokatska komora, Komitet za zaštitu privatnosti I borbu protiv kompjuterskog kriminala, Odjeljenje za načno i tehnološko pravo. Branko Stamenković, Adis Balota ''Visokotehnološki kriminal-praktični vodič kroz savremeno krivično pravo i primjere iz prakse''ISBN 978-9940-500-15-3 Dr Miroslav Bača, ''Uvod u računalnu sigurnost'' Narodne novine, Zagreb 2004.godina. www.first.org www.isoc.org

	www.w3c.org Scripts from lectures and seminars
Other remarks	

Course name	***Digital Forensics of Mobile Phones***
Course description (1 sentence)	Major part of digital forensics refers to computer system forensics, whether computers are standalone or networked, and to mobile phone forensics Digital forensics involves scientific data testing and analysis from mobile phones memory and Cloud, and from systems and other data storage media and spaces in mobile communication devices, so that data can be used as evidence in court
ECTS	6
Lectures (hours)	30
Labs (hours)	16
Seminars (hours)	16
Individual work (hours)	60
Prerequisites	
Objectives	The objective of this course is that students learn the basic principles and requirements of digital forensic analysis of mobile communication devices. By understanding the nature of digital records, hardware functionality of mobile telephony devices, basic principles of tools used in mobile telephony forensics, students are trained to self-recover hidden data in a mobile phone by applying forensic techniques and tools
Teaching and learning methods	Lectures, seminars, labs.
Course content (topics covered)	• Introduction to digital forensics. • Data gathering and searching. Legislation. • Data analysis and presentation. Legislation. Forensic tools. • Digital forensics of computer system. Computer hardware components. • Concept of mobile telephony • Cellular approach to the Internet • Security mechanisms in mobile telephony • Mobile phone hardware and software XRY and UFED – Cellebrite forensic tools Smart phones forensics. • Mobile devices' data extraction • Data acquisition and their analysis • CLOUD data acquisition and their analysis • Case studies
Learning outcomes	
Students responsibilities	Students have to attend lectures and seminars. They do project assignments, midterm exams, and final exam.

Assessment	The exam consists of mid-term exams I and II, seminar paper and final exam which may be written or oral. In order to pass the exam, a student has to gain minimum 51% points on mid-term exams I and II and on final exam and project assignment. The final grade is formed after summarizing the points for pre-exam and exam assignments. - Mid-term exam I - 20 points - Project work I revision – 5 points - Mid-term exam II - 20 points - Project work I revision – 5 points - Final exam consists of oral presentation and demonstration of final project information system - 50 points In order to pass the exam, a student has to accumulate minimum 51 points. In accordance with the Rules on grading and accumulated points, final grade will be formed as follows: • 0-50 F • 51-59 E • 60-69 D • 70-79 C • 80-89 B • 90-100 A
Literature	Barrett, D., Kipper, G., Virtuelization and Forensics a digital forensic investigator's guide to virtel environments, Elsevier Inc., Burlington, MA 01803, USA, 2010. M.Milosavljević, G. Grubor , Digitalna forenzika računarskih sistema, Univerzitet Singidunum, 2009. Reyes, A. Cyber Crime Investigations: Digital Forensics and Analysing Data. Rockland: Syngress Publishing Inc., 2007. http://mobileforensics.files.wordpress.com Scripts from lectures and seminars
Other remarks	