UNIVERZITET METROPOLITAN BEOGRAD

MASTER STUDIES

INFORMATION SECURITY

INFORMATION SECURITY

> Program duration: 1 year
> ECTS number: 60 ECTS
> Academic Title: Master of Computer Science
> Field of Study: Natural Sciences and Mathematics
> Domain: Computer Science
> Forms of Studying: Online, via Internet (eLearning system)

PROGRAM DESCRIPTION

This program focuses on studying of some of the most relevant aspects of Information Security. It deals with security aspects from a network layer to an application layer, and it gives the comprehensive understanding of the concept of security and its implications on computer networks, databases, web service infrastructure and software design. Special research areas include (but are not limited to) the best practice in the computer networks security and operating system security, database security and security in software engineering, compromised computer systems, detection and defense methods, cryptography and crypto-technologies, web application security and computer forensics.

Study program of Master Academic Studies in Information Security educates students to work on security development and implications of computer networks, databases, web service infrastructure and software design, all from an aspect of information security and systems with detection and defense methods, cryptography and crypto-technologies, web application security and computer forensics.

This study program provides an acquisition of competencies which are socially justified, useful and in line with the tasks and objectives of the University at which the study program is carried out. The purpose of this study program is to provide students with solid theoretical foundation necessary for essential understanding of the problem of information security and information systems security, as well as to enable them for rational and professional performance of various practical activities and tasks which are associated with their profession. The outcome of these activities and tasks is the identification of needs and demands, and its fulfillment provides the full functionality of information security and defining all modules and components with the projection of complex information security systems.

As a result of the ImprESS project of the Erasmus + program funded by the European Union, three new cases have been developed.

THE OUTCOMES OF STUDYING AT THE STUDY PROGRAM

The acquired knowledge will enable the student to obtain the following job professions:

> A digital forensic expert,
> A computer architecture expert in secure systems and networks,
> A controller and expert in testing and revision of the security components of the system,
> An analyst of the systems or network security,
> A consultant for computer security in corporate and state organizations,
> A technical security director in different types of organizations,
> A leading computer scientist in the field of information security,
> An expert participating in the development of software or information systems from the standpoint of information security (security software engineering),
> A training instructor for personnel of oraganizations in the field of security practice dealing with information systems and information security solutions.

SEMESTER	NUMBER	MSc **INFORMATION SECURITY** (60 ECTS, 1 YEAR)	ECTS	LECTURE HOURS	TUTORIAL HOURS
1	1	CS470 **Cryptography and Crypto Technologies**	8	2	3
	2	CS471 **Operation Systems Security**	8	2	3
	3	CS472 **Computer Networks Security**	8	2	3
	4	CS571 **Computing Forensics**	8	2	3
2	5	CS535 **Ethics and Data Privacy**	8	2	3
	6	**Elective course**			
	7	CS595 **Capstone CS Project**	12	0	0

		ELECTIVE COURSES			
2	6	CS545 **Cyber Security with Blockchain**	8	2	3
	6	CS530 **Information Security Management**	8	2	3
			ECTS: 60		

PROGRAM ORGANIZATION

Mandatory Courses

CS470 Cryptography and Crypto-Technology
CS471 Operating System Security
CS472 Computer Networks Security
CS571 Computing Forensics
CS535 Ethics and Data Privacy
CS595 Završni rad

Elective Course 1 (1 subject is selected)

CS545 Cyber Security with Blockchain
CS530 Information Security Management

COURSES SHORT DESCRIPTION

CS470 Cryptography and Crypto Technologies

Students are conversant with the concept of cryptography studies. They are introduced to different types of cryptosystems and basic levels of cryptanalytic attacks. The course deals with basics of modular arithmetic, the theory of numbers and the overview of algorithms for the factorization of large numbers. This way, students acquire necessary mathematical knowledge used in cryptography. Students are conversant with the basic characteristics of block cypher cryptography systems with and without the key, as well as techniques for forming digital signature and key exchange. Teaching units within the course: Classical cryptography (the history of cryptography, basic concepts, types of cryptography systems), Classical cryptography techniques (substitution ciphers, transposition ciphers and encrypters), Mathematical basics (Modular arithmetic, Euclid's algorithm, Finite field, ECC, Group, ring and field), block ciphers and DES, AES, Symmetric algorithms – Symmetric cryptography, Pseudorandom number generators and Stream ciphers, Public key cryptography, asymmetric cryptography, RSA and Elgamal algorithm, key management, Hash functions, MAC and HMAC algorithms, PKI, steganography and cryptanalysis (Models and characteristics of cryptanalysis).

CS471 Operation Systems Security

Students are conversant with the concept of operating systems. The objective of the course is to enable students to continue their studies in the field of the application software security, computer systems and networks, as well as gain qualifications for dealing with problems related to protection form cyber attacks and information security. Students are conversant with the basic concepts of OS security, memory protection, multitasking, system installation and the administration of the operating system itself. Teaching units within the course: The basics of computer hardware through RUN time of a program, Operating system of zero protection such as CPM, MSDOS, OS without protection), Memory protection and multitasking virtualization concept, Virtual operating systems, Improving operating systems, Initialization of an operating system, Database access control, System activity monitoring, OS installation, editing and updating , System backup.

CS472 Computer Networks Security

The course deals with different aspects of network security. Mastering this course and the ability of applying the acquired knowledge after the completion of the course are necessary for understanding other courses within the study program. The objective of this course is to introduce students to the basic concepts and components necessary for the protection of networks, such as firewalls, routers, switchers, intrusion detection and protection systems, and logging infrastructures. During the semester students implement a project on analysis and usage of critical components of network security. This way students will prepare for further improvement in the field of network security. Teaching units within the course: At the beginning of the course, students will be conversant with the basic network tools, OSI model and ICMP protocol. They will also be conversant with a Proxy firewall, DMZ, IPS and IDS. They will also learn about packet filtering, dynamic packet filtering (ACL-RACL), IPTABLES commands, virtual private networks and wireless network security.

CS571 Computing Forensics

The objective of the course is that students prepare for research in the field of systematic control of a computer system and its content, with the aim of data gathering in case of a crime or other malpractice the computer is used for. After the completion of the course students will be able to understand the role of computer forensics in criminal investigations, they will also be able to apply the process of forensic analysis (finding and identifying digital proofs; storing digital proofs; analysis; presenting analysis results). Teaching units within the course: The basics of digital research (data analysis and the world of incidents). Analysis of permanent memory and analysis of permanent memory based on division. Analysis of system data files (FAT and NTFS concepts). NTFS concept and date structure, UFS and BSDFS concepts and analysis. Forensics of data storage devices based on the Linux platform. Mobile phones forensics, android forensics and forensics of PDA devices. Log files processing, Forensic tools used in investigations, Cybercrime Law and Criminal Law in the Republic of Serbia.

CS535 Ethics and Data Privacy

Ethics is part of a research project, from the phase of research topic suggestion to the end of the research project. Based on the data that is obtained, it is necessary to follow different regulations, such as regulations in the field of intellectual property, regulations in the field of protection of personal data, particularly General Data Protection Regulation (GDPR). Data security can be at risk by illegal access to vulnerable data, data change or other types of malpractice. The course deals with basic postulates of ethics in the field of data security, ethical, social and legal aspects of software development, organizational, security and legal issues in the field of data protection, as well as digital contracts.

CS545 Cyber Security with Blockchain

The objective of the course is that students become conversant with the concept of blockchain technology in the context of information security, current security policy on the Internet, vulnerabilities of modern computer systems and technologies and attacks. The course enables students to recognize security problems related to blockchain technology and to find out how to achieve protection from attacks and how to protect information by using adequate mechanisms. After they successfully complete the teaching units and assignments within the course curriculum, students are expected to be able to apply acquired knowledge in practice. Teaching units within the course: Distributed systems and blockchain technology, consensus mechanisms in blockchain technology, smart contracts, symmetric cryptography, asymmetric cryptography, blockchain and Internet of things, current security attacks on systems, security ecosystem, blockchain security – confidentiality, integrity, availability, public key infrastructure, authentication by application of blockchain, blockchain as DNS server, blockchain against distributed DoS attacks.

CS530 Information Security Management

Students will be conversant with the concept of security system management. The objective of the course is to enable students for further studies in the field of information security management system (ISMS), risk management as well as qualifications for professional work on ISO27000 standards implementing. Students are introduced to basic concepts of ISMS, its audit, management, operations, as well as its certification and development. Teaching units within the course: The basics of ISMS family, ISMS risk management, Risk management controls, ISMS operations, Performance evaluation, Accredited ISMS certification, Property management, Communications and operations management, Controls against malware and backup copies and network security management and media management, Information exchange and access control, Network access control and cryptography controls, as well as business continuity management, agreement and audit.

CONTACT AND LOCATION

Online learning, within 1 year with a master's degree.
Skip the competition and take it to the next level of his career.

Contact us,
we will be happy to answer your questions:

Univerzitet Metropolitan
Tadeuša Košćuška 63
11000 Beograd
Tel: +381 (11) 203 08 85
     +381 (69) 203 08 85
Faks: +381 (11) 203 06 28
email: info@metropolitan.ac.rs
www.metropolitan.ac.rs

We are waiting for you!