MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU
MEĐIMURJE UNIVERSITY OF APPLIED SCIENCES IN ČAKOVEC

COURSE SYLLABUS

ACADEMIC YEAR: 2025/2026

1. GENERAL COURSE INFORMATION

1.1 Course name	**Security of computer networked systems**			
1.2 Study program/s	UNDERGRADUATE PROFESSIONAL STUDY PROGAMME COMPUTER ENGINEERING			
1.3 Course status (O,E)	E	**1.6 Mode of instruction (number of hours)**	**Lectures**	30
1.4 Course code			**Exercises**	30
1.5 Course abbreviation			**Seminars**	
1.6 Semester	V		**E-learning**	Merlin
1.7 ECTS	5	**1.7 Place and time of instruction**	The premises of the Međimurje University of Applied Sciences in Čakovec, according to the schedule published on the website	

2. TEACHING STAF.F

2.1 Course leader/s-title	Jurica Trstenjak, senior lecturer	**contact**	jtrstenjak@mev.hr
		contact	
2.2 Assistant/s- title		**contact**	
		contact	
2.3 Instruction held by- title	Jurica Trstenjak, senior lecturer	**contact**	jtrstenjak@mev.hr
2.4 Course leader/s-title		**contact**	

3. COURSE DESCRIPTION

3.1. Course goals	Introduction to basic threats to computer systems and computer networks. Mastering the basic mechanisms for protection against attacks. Meeting with system architectures, protocol architectures, protocols, and security enhancement tools.
3.2 Prerequisites	Passed Computer Network course.
3.3 Course outcomes	After successfully completing the course, students will be able to: O1 - explain basic concepts and concepts related to computer security O2 - describe the types of security threats and attacks and the most common methods of defense O3 - Explain ways for remote access (SLIP, PTP, "tunneling", wireless protocol, RADIUS, TACACS), ways to establish a secure connection O4 - List and explain attacks on DNS servers and how to protect yourself and how to improve the protection of network devices (routers and network barriers) O5 - Explain EAP messaging, Request / Response packet type, Sucess / Failure packet type and EAP-TLS O6 - List and explain the basic algorithms for data encryption (DES, 3DES, RIJNDAEL, RSA, RC4, VIGENERE and HASH function)
3.4 Contribution of the course to the study program	Use English in the domain of ICT in communication with experts and lay people. Analyze user needs (research and detect data sources, currently present business systems, technological limitations, specifics of the business environment).

	Apply standards, methods and techniques to analyze security threats and combat threats.
3.5 Course content	Basic goals of the data protection system. Identification. Protection topology. Risk evaluation. Attacks. Viruses. Elements account. networks and connectivity. Network barriers, routers, switches. Remote access. Online traffic monitoring. Unauthorized intrusions into wireless networks. EAP protocol and methods. Encryption algorithms.

3.6 Types of coursework

x	Lectures	X	Exercises		Blended e-learning		Individual activities	x	Laboratory
	Seminars and workshops		Distant learning		Field classes	x	Multimedia and network		Mentorship
	Other								

3.7 Language of instruction	Croatian

3.8 Monitoring students' work (enter the number of ECTS credits for each activity so that the total number of ECTS credits is equal to the total ECTS value of the course, 1 ECTS = 30 hours)

2	Class attendance		Seminars		Research
2,5	Midterm exams/written exam		Project		Essay
0,5	Oral exam		Practical task		

Activity specification	Percent %	Points
Assessment during instruction		
Lesson assignments	10%	10
Midterm exam 1	30%	30
Midterm exam 2	30%	30
Oral exam	15%	15
Practical task	15%	15
Exam assessment for the students who failed to fullfil all the obligatory requirements during the semester		
Written exam	60%	60
Oral exam	15%	15
Total:	**100%**	**100**

Points Grade
89 – 100 excellent (5)
76 – 88 very good (4)
63 – 75 good (3)
50 – 62 pass (2)
0 – 49 fail (1)

3.9 Specific features related to taking the course	*If a student collects 50% of the points of each outcome he/she directly accesses the oral exam. If a student does not achieve a sufficient number of points on the midterm exam, he/she cannot take the next midterm exam, and has to take the written exam.* *If he/she passes the written exam, he/she will proceed to the oral part of the exam.* *The seminar paper is submitted within the agreed deadline, and certainly before the exam term.* *The final grade is given on the oral part of the exam.*
3.10 Students obligations	• a full-time student has the right to sit for the exam if he attends classes for a minimum of 70% of the total prescribed number of hours • a full-time student who attends classes from 50 to 70% of the total prescribed number of hours can exercise the right to take the exam

	by completing additional teaching activities in agreement with the course teacher • a full-time student who attends a certain course for less than 50% of the prescribed number of hours enrolls in the course the following academic year • a part-time student has the right to sit for the exam if he/she attends classes for a minimum of 30% of the total prescribed number of hours • a part-time student who attends classes for 20 to 30% of the total prescribed number of hours can exercise the right to sit for the exam by completing additional teaching activities in agreement with the course teacher • a part-time student who attends the classes of a certain course for less than 20% of the prescribed number of hours re-enrolls in the course the following academic year
3.11 Written assignments	
3.12 Required reading	
3.13 Additional reading	*Kaufman C., R. Perlman, M. Speciner: Network Security: Private Communication in a Public World, 2nd edition, Pearson Education, 2002.*

4. ADDITIONAL INFORMATION ABOUT THE COURSE	
4.1 Quality control	The quality of the program, teaching process, teaching skills and level of mastery of the material will be established by conducting a written evaluation based on questionnaires, and in other standardised ways and in accordance with the by-laws of the Međimurje University of Applied Sciences in Čakovec.
4.2 Contact the teacher	Students can contact the teacher during the office hours and during classes. All other methods of communication are arranged with the teacher. It is also possible to ask questions by e-mail, which will be answered in 48 hours at the latest. It is desirable for students to come as often as possible for any possible questions during the teacher's office hours.
4.3 Information about the course	It is the obligation of each student to be regularly informed about the course. All notifications about the classes or possible postponement of classes will be posted on the bulletin board and on the website of the University at least 24 hours in advance.

5. ELABORATION OF THEMATIC UNITS

Week	Topic	Course outcome
1.	Introduction, basic concepts of the protection system	O1
2.	Risk assessment, how to recognize attacks, TCP/IP protocol (problem of protection)	O1, O2
3.	Infrastructure and connectivity (network barriers, routers, VPN, switches)	O1, O2
4.	Remote access, protection of Internet connections	O2, O3
5.	Monitoring of network traffic, attack detection systems	O2, O4
6.	Monitoring of network traffic, attack detection systems	O2, O4
7.	Security of wireless networks	O2, O3
8.	1st midterm exam	
9.	Implementation and maintenance of a protected network	O3, O4
10.	Network and work environment protection	O4
11.	Extensible authentication protocol	O5
12.	Extensible authentication protocol	O5
13.	Encryption algorithms	O6
14.	Email and Web Security	O4, O6

15.	2nd midterm exam + oral part	