

Subject card

Subject name and code	Cybersecurity, PG_00156476						
Field of study	Cybersecurity						
Date of commencement of studies	October 2024		Academic year of realisation of subject		2025/2026		
Education level	Master's studies		Subject group		Obligatory subject group in the field of study Subject group related to scientific research in the field of study		
Mode of study	full-time studies		Mode of delivery		at the university		
Year of study	2		Language of instruction		English		
Semester of study	4		ECTS credits		7.0		
Learning profile	academic		Assessment form		exam		
Conducting unit	Department of Business Informatics -> Faculty of Management -> Rector						
Name and surname of lecturer (lecturers)	Subject supervisor		dr inż. Przemysław Jatkiewicz				
	Teachers						
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	0.0	45.0	0.0	0.0	60
	E-learning hours included: 0.0						
Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan		Participation in consultation hours		Self-study	SUM
	Number of study hours	60		30.0		85.0	175
Subject objectives	To familiarise students with the processes, good practices and technology solutions that facilitate the protection of critical systems and networks from digital attacks.						

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[IiEMU2_W05] The student has an in-depth knowledge of socio-economic data sources, their databases and how to create them.	Knows the risks of information systems and their impact on the enterprise and society.	[SW4] test/egzamin - ustny lub pisemny
	[IiEMU2_W07] The student has an extended and established knowledge of ethical norms applicable to business, good practices for its conduct and legal regulations for the protection of intellectual property. The student has an extended knowledge of the risks and responsibilities associated with the computerization of business processes. The student knows the principles of netiquette.	Is familiar with the legal and ethical considerations of information systems testing.	[SW4] test/egzamin - ustny lub pisemny
	[IiEMU2_U08] The student can analyse business needs and, as appropriate, configure and apply modern information and communication technologies in business management and business communication.	Can select appropriate safeguards for indicated vulnerabilities.	[SU5] realizacja zadania problemowego
	[IiEMU2_K03] The student is able to communicate freely with the public inside and outside the workplace, transfer his knowledge and share his skills through various media.	Knows and can use the communication channels dedicated to reporting cyber security incidents.	[SK5] realizacja zadania problemowego
	[IiEMU2_U04] The student is able to plan, design, and program information systems at an advanced level, supporting the operation of business entities.	Can implement appropriate security measures for the vulnerabilities identified	[SU5] realizacja zadania problemowego
	[IiEMU2_K06] The student knows the need for ethical, sustainable and socially responsible behavior in professional and social life. Initiates and organises activities for the social environment and public interest.	Is aware of the dangers of navigating cyberspace.	[SK5] realizacja zadania problemowego
Subject contents	Regulations, standards, good practices related to cyber security. Personal data protection Threats and vulnerabilities to information systems Physical security of servers Malware Audit, control, tests, checks Risk analysis methodologies Cryptography Familiarise students with the principles of protecting LAMP servers (Linux, Apache, Mysql, PHP). Identification. Authentication, authorization. Server protection against malware Planning and preparation of an audit, conducting an audit, post-audit activities Audit support tools Conducting a risk analysis		
Prerequisites and co-requisites	No		
Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	completion of a problem task	51.0%	50.0%
	test/examination - oral or written	51.0%	50.0%
Recommended reading	Basic literature	P. Jatkiewicz ,Security of information systems of companies and institutions UG 2020 R.R. Moeller, IT audit, control, and security John Wiley & Sons 2010	
	Supplementary literature	E. Nemeth, G. Snyder, T. Hein, B. Whaley, UNIX and Linux System Administration Handbook, Pearson Education 2017	
	eResources addresses		
Example issues/ example questions/ tasks being completed	Protect the specified application against a sqlinjection attack		

Work placement	Not applicable
----------------	----------------

Document generated electronically. Does not require a seal or signature.