University of Gdańsk

Subject card

Subject name and code	Cybersecurity, PG_00156502						
Field of study	Cyberbezpieczeństwo						
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	Polish			
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_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_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 safeguards for identified vulnerabilities.	[SU5] realizacja zadania problemowego
[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 analyse business needs and, as appropriate, configure and apply modern information and communication technologies in the process of business management and business communication. Be able to select appropriate security measures for identified vulnerabilities.	[SU5] realizacja zadania problemowego
[IiEMU2_K02] The student can communicate freely with the public on specialised topics in the field of computer science and econometrics in and outside the workplace, communicate his knowledge and share his skills through various media. Culturally participates in discussions, is not afraid to ask questions and knows how to give constructive criticism.	Knows and can use the communication channels dedicated to reporting cyber security incidents.	[SK5] realizacja zadania problemowego
[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_K05] The student can think and act in an entrepreneurial manner and flexibly adapt to changing environmental conditions. Thinks creatively and can go beyond the usual patterns.	Is aware of the dangers of moving around in cyberspace	[SK5] realizacja zadania problemowego

Subject contents

Regulations, standards, good practices related to cyber security. Personal data protectionThreats and vulnerabilities to information systemsPhysical security of serversMalwareAudit, control, tests, checksRisk analysis methodologiesCryptographyFamiliarise students with the principles of protecting LAMP servers (Linux, Apache, Mysql, PHP).Identification. Authentication, authorization.Server protection against malwarePlanning and preparation of an audit, conducting an audit, post-audit activitiesAudit support toolsConducting a risk analysis

Prerequisites and co-requisites

No

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
test/examination - oral or written	51.0%	50.0%
completion of a problem task	51.0%	50.0%

Recommended reading

Basic literature	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	Secure the indicated application against a sqlinjection attack.	
Work placement	Not applicable	

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