GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	CYBERSECURITY MANAGEMENT, PG_00061870		
Field of study	Engineering Management		
Date of commencement of studies	October 2024	Academic year of realisation of subject	2026/2027
Education level	first-cycle studies	Subject group	Optional subject group Subject group related to scientific research in the field of study
Mode of study	Part-time studies	Mode of delivery	at the university
Year of study	3	Language of instruction	Polish
Semester of study	6	ECTS credits	3.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department Of Informatics In Management -> Faculty Of Management And Economics -> Wydziały Politechniki Gdańskiej		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. inż. Rafał Leszczyna	
	Teachers		

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	8.0	0.0	8.0	0.0	0.0	16

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	16	6.0	53.0	75

Subject objectives

Analyzes and critically assesses threats to cybersecurity of the company's IT resources, designing appropriate protection measures

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K6_U07] applies information technology to improve critical analysis and evaluation of data and management processes	critically assesses the problems of cybersecurity threats in the enterprise and defines appropriate protection measures	[SU3] Assessment of ability to use knowledge gained from the subject
[K6_W03] identifies reliable sources of information relevant to the analyzed issues	analyzes the enterprise and its IT resources, identifying cybersecurity threats	[SW1] Assessment of factual knowledge

Subject contents

Basic concepts and concepts of cyber security
Usable cybersecurity
Cybersecurity management proces
Cybersecurity risk management
Cyber security threats
Selected standards and guidelines for cybersecurity
Security

Prerequisites and co-requisites

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Active participation in the lecture	60.0%	5.0%
Knowledge test	60.0%	45.0%
Laboratory exercises	60.0%	50.0%

Recommended reading

Basic literature

ISO/IEC 27001:2017
NIST SP 800-53 Revision 5
Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014
Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html
David Kennedy, Jim OGorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011

	Supplementary literature	Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001 Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 ISO/IEC 15408 (Common Criteria) Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017
	eResources addresses	Adresy na platformie eNauczanie:
Example issues/ example questions/ tasks being completed	Perform an enterprise analysis. Identify and describe its cyber resources Identify independent cybersecurity risk lists and develop your own cyberthreat list Estimate your cybersecurity risk Explain a systematic approach to enterprise cybersecurity management Choose a cybersecurity standard, justify your choice Give an example of a violation of the integrity of a cyber resource Give an example of a security measure to reduce the risk of accounting data being copied by unauthorized users Provide and explain the formula for cybersecurity risk Point out and explain the most common strategies for dealing with cybersecurity threats Describe the basic features of access control	
Work placement	Not applicable	

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