GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	CYBERSECURITY MANAGEMENT, PG_00056590		
Field of study	Engineering Management		
Date of commencement of studies	October 2020	Academic year of realisation of subject	2023/2024
Education level	first-cycle studies	Subject group	Optional subject group 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	4	Language of instruction	English
Semester of study	7	ECTS credits	3.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Informatics in Management -> Faculty of Management and Economics		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. inż. Rafał Leszczyna	
	Teachers	dr hab. inż. Rafał Leszczyna	

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	15.0	0.0	15.0	0.0	0.0	30

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	30	0.0	0.0	30

Subject objectives

For a student to acquire the fundamental knowledge on cybersecurity management in organisations.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K6_W13] has a basic knowledge of the design, modelling and optimisation of technical processes and systems	Student: - describes an enterprise, - identifies and describes cyberassets, - recognizes and describes cybersecurity problems in enterprises, - defines protection measures.	[SW1] Assessment of factual knowledge [SW3] Assessment of knowledge contained in written work and projects
[K6_U08] analyses engineering and managerial solutions in decision-making processes, taking into account pro-quality and pro-environmental aspects, as well as safety of work processes	Student: - analyses an enterprise and its cyberassets, - analyses cybersecurity threats, - selects protection measures.	[SU1] Assessment of task fulfilment [SU2] Assessment of ability to analyse information

Subject contents

- Basic concepts, fundamentals of cybersecurity
- Usable cybersecurity
- Cybersecurity management process
- Cybersecurity risk management
- Cybersecurity threats
- Selected cybersecurity standards and guidelines
- Protection controls

Prerequisites and co-requisites

Communicative English

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
knowledge examination	60.0%	45.0%
lab exercises	60.0%	50.0%
active participation in the course meetings	60.0%	5.0%

Recommended reading	Basic literature	1. ISO/IEC 27001:2017 2. NIST SP 800-53 Revision 5 3. Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014. 4. Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html 5. David Kennedy, Jim OGorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011.
	Supplementary literature	1. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001 2. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 3. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 4. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 5. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 6. ISO/IEC 15408 (Common Criteria) 7. Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017
	eResources addresses	Adresy na platformie eNauczanie: Cybersecurity Management - 2023 - Moodle ID: 27258 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=27258
Example issues/ example questions/ tasks being completed	1. Analyse an enterprise. Identify and describe its cyberassets. 2. Identify independent lists of cybersecurity threats and develop your proprietary list of cyberthreats. 3. Calculate cybersecurity risks. 4. Explain a systematic approach of cybersecurity management in an enterprise. 5. Choose a cybersecurity standard, justify the choice. 6. Provide an example of violating the integrity of a cyberasset. 7. Provide an example of a security control to reduce the risk of copying accounting data by unauthorised users. 8. Provide and explain the cybersecurity risk formula. 9. Enlist and explain the most common cybersecurity risk treatment strategies. 10. Describe principal characteristics of access control.	
Work placement	Not applicable	