GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	CYBERSECURITY MANAGEMENT, PG_00070697		
Field of study			
Date of commencement of studies	October 2026	Academic year of realisation of subject	2028/2029
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	3	Language of instruction	English
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 -> Faculties of Gdańsk University of Technology		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. inż. Rafał Leszczyna	
	Teachers		

Lesson types

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	15.0	0.0	30.0	0.0	0.0	45

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	45	3.0	27.0	75

Subject objectives

Preparing students for independent identification and analysis of cybersecurity threats and for designing appropriate protective measures, based on knowledge of risk management as well as the main concepts, processes, and standards of cybersecurity management, and shaping attitudes related to the responsible use of technologies in the context of organizational cybersecurity.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K6_W03] knows reliable sources of information and utilizes advanced knowledge to explain contemporary management issues.	knows and understands reliable sources of information, concepts and processes of cybersecurity management, as well as standards (e.g., ISO/IEC 27001, NIST), in the context of threat analysis and the selection of appropriate security measures for enterprise information systems	[SW2] Assessment of knowledge contained in presentation
[K6_U06] acquires specialized knowledge in the field of engineering management, demonstrating the ability to effectively plan individual work and pursue lifelong learning.	is able to analyse an organisation’s cyber assets, identify potential threats, and propose appropriate risk mitigation measures using available tools and management methodologies.	[SU3] Assessment of ability to use knowledge gained from the subject [SU5] Assessment of ability to present the results of task
[K6_K01] is ready to fulfill professional roles responsibly, taking legal, ethical, and cultural aspects into account in decision-making processes.	is ready to make responsible decisions in the field of cybersecurity, taking into account legal, ethical, and social implications, especially regarding data protection and privacy	[SK3] Assessment of ability to organize work [SK5] Assessment of ability to solve problems that arise in practice

<table>
<tr><td>Subject contents</td><td>Course content – lecture
1. Basic concepts and concepts of cyber security
2. Usable cybersecurity
3. Cybersecurity management proces
4. Cybersecurity risk management
5. Cyber security threats
6. Selected standards and guidelines for cybersecurity
7. Security
Course content – laboratory
1. Basic concepts and concepts of cyber security
2. Usable cybersecurity
3. Cybersecurity management proces
4. Cybersecurity risk management
5. Cyber security threats
6. Selected standards and guidelines for cybersecurity
7. Security</td></tr>
<tr><td>Prerequisites and co-requisites</td><td></td></tr>
<tr><td>Assessment methods and criteria</td><td>
<table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td>Case study</td><td>60.0%</td><td>50.0%</td></tr>
<tr><td>Written knowledge test with closed and open-ended questions</td><td>60.0%</td><td>45.0%</td></tr>
<tr><td>Substantive participation during the lecture</td><td>60.0%</td><td>5.0%</td></tr>
</table>
</td></tr>
<tr><td>Recommended reading</td><td>
<table>
<tr><td>Basic literature</td><td>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</td></tr>
<tr><td>Supplementary literature</td><td>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</td></tr>
<tr><td>eResources addresses</td><td></td></tr>
</table>
</td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td>• 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</td></tr>
<tr><td>Practical activites within the subject</td><td>Not applicable</td></tr>
</table>

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