GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Cybersecurity Management, PG_00068300		
Field of study			
Date of commencement of studies	October 2025	Academic year of realisation of subject	2027/2028
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	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		
	Teachers		

Lesson types and methods of instruction

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	5.0	25.0	75

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_K01] is ready to fulfill professional roles responsibly, taking legal, ethical, and cultural aspects into account in decision-making processes.	is able to make thoughtful decisions regarding the protection of information and digital infrastructure, considering the legal, social, and organizational implications of actions in the digital environment	[SK5] Assessment of ability to solve problems that arise in practice
[K6_W03] knows reliable sources of information and utilizes advanced knowledge to explain contemporary management issues.	is familiar with approaches and information sources that support understanding of key digital security challenges in organizations and can analyze their impact on modern management structures	[SW3] Assessment of knowledge contained in written work and projects
[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 independently seek out and update knowledge related to digital security threats and practices, effectively planning personal development in response to evolving technological realities	[SU5] Assessment of ability to present the results of task [SU3] Assessment of ability to use knowledge gained from the subject

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

<table>
<tr><td>Assessment methods and criteria</td><td colspan="2"><table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td>lab exercises</td><td>60.0%</td><td>50.0%</td></tr>
<tr><td>active participation in the course meetings</td><td>60.0%</td><td>5.0%</td></tr>
<tr><td>knowledge examination</td><td>60.0%</td><td>45.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Recommended reading</td><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>Adresy na platformie eNauczanie:</td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td colspan="2">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.</td></tr>
<tr><td>Work placement</td><td colspan="2">Not applicable</td></tr>
</table>

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