



Subject card

Subject name and code	CYBERSECURITY MANAGEMENT, PG_00056981						
Field of study	Engineering Management						
Date of commencement of studies	October 2019	Academic year of realisation of subject			2022/2023		
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	4	Language of instruction			Polish		
Semester of study	8	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	8.0	0.0	8.0	0.0	0.0	16
	E-learning hours included: 0.0						
Zarządzanie cyberbezpieczeństwem - niestacjonarne 2023 - Moodle ID: 27732 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=27732							
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		0.0		0.0	16
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: - identifies and describes cyberassets, - recognizes and describes cybersecurity problems in enterprises, - defines protection measures.		[SW3] Assessment of knowledge contained in written work and projects [SW1] Assessment of factual knowledge		
[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.		[SU2] Assessment of ability to analyse information [SU1] Assessment of task fulfilment			
Subject contents	<ul style="list-style-type: none">• Basic concepts, fundamentals of cybersecurity• Information Security Management System• Cybersecurity risk management• Protection controls• Standard ISO/IEC 27001• ISO/IEC 27001-based cybersecurity management process• Security policy• Cybersecurity threats						
Prerequisites and co-requisites	English proficiency in reading						
Assessment methods and criteria	Subject passing criteria		Passing threshold		Percentage of the final grade		
	lab exercises		60.0%		50.0%		
	activeness during lecture		60.0%		5.0%		
	knowledge examination		60.0%		45.0%		

Recommended reading	Basic literature	<ol style="list-style-type: none"> 1. ISO/IEC 27001:2018 2. Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014. 3. Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html 4. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011.
	Supplementary literature	<ol style="list-style-type: none"> 1. NIST SP 800-53 Revision 5 2. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001 3. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 4. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 5. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 6. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 7. ISO/IEC 15408 (Common Criteria) 8. Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017
	eResources addresses	<p>Uzupełniające</p> <p>https://cyberdefence24.pl/cyberbezpieczenstwo - cyberdefence24.pl portal</p> <p>https://www.gov.pl/web/baza-wiedzy - gov.pl knowledge base</p> <p>https://www.nist.gov/topics/cybersecurity - NIST cybersecurity resources</p> <p>https://www.schneier.com/ - Bruce's Schneier blog</p> <p>https://www.cert.pl/ - CERT NASK portal</p> <p>https://www.enisa.europa.eu/ - ENISA</p> <p>https://niebezpiecznik.pl/ - Portal https://niebezpiecznik.pl/</p>
Example issues/ example questions/ tasks being completed	<ol style="list-style-type: none"> 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. Provide an example of violating the integrity of a cyberasset. 5. Provide an example of a security control to reduce the risk of copying accounting data by unauthorised users. 6. Provide and explain the cybersecurity risk formula. 7. Enlist and explain the most common cybersecurity risk treatment strategies. 	
Work placement	Not applicable	