



Subject card

Subject name and code	Cybersecurity of Enterprise Infrastructure, PG_00053095						
Field of study	Data Engineering						
Date of commencement of studies	October 2020	Academic year of realisation of subject			2022/2023		
Education level	first-cycle studies	Subject group			Obligatory subject group in the field of study Subject group related to scientific research in the field of study		
Mode of study	Full-time studies	Mode of delivery			blended-learning		
Year of study	3	Language of instruction			English		
Semester of study	6	ECTS credits			3.0		
Learning profile	general academic profile	Assessment form			exam		
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 inż. Sławomir Ostrowski dr hab. inż. Rafał Leszczyna					
Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	30.0	0.0	30.0	0.0	0.0	60
	E-learning hours included: 16.0						
	Cybersecurity of Enterprise Infrastructure 2023 - Moodle ID: 20658 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=20658						
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	60	6.0		9.0		75
Subject objectives	The aim of the course is for a student to acquire knowledge in the area of cybersecurity management in enterprise IT infrastructures.						
Learning outcomes	Course outcome	Subject outcome			Method of verification		
	[K6_W04] Knows the architecture of computers, operating system processes, file systems, text processing programs, disk and ram memories management rules. Knows the problems of sharing the state, presentation and transformation of information in a distributed system, hypermedia technologies and related services, the architecture of interactive distributed simulation and agent interaction methods.	Student: - describes IT infrastructure of an enterprise, - identifies the enterprise IT infrastructure assets, - recognises IT security problems in enterprises, - defines protection measures.			[SW3] Assessment of knowledge contained in written work and projects [SW1] Assessment of factual knowledge		
	[K6_U02] designs, analyses correctness and creates functional specification of IT systems, selects appropriate measures, creates quality models, prepares and assesses their design documentation.	Student: - analyses IT infrastructure of an enterprise, - assesses the cost related to security of the IT infrastructure, - 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• Usable cybersecurity• Cybersecurity management system• Cybersecurity standards and guidelines• Cybersecurity management process• Cybersecurity policy• Cybersecurity threats• Risk management• Cybersecurity controls• Cost of the cybersecurity management						

Prerequisites and co-requisites	Communicative English		
Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	Active participation during the lectur	0.0%	5.0%
	Knowledge examination	60.0%	45.0%
	Laboratory exercises	60.0%	50.0%
Recommended reading	Basic literature	<ol style="list-style-type: none"> 1. ISO/IEC 27001:2013 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 Second 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	<ol style="list-style-type: none"> 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	<p>Uzupełniające</p> <p>https://cyberdefence24.pl/cyberbezpieczenstwo - cyberdefence24.pl portal</p> <p>https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber-gov.pl cybersecurity knowledge base</p> <p>https://niebezpiecznik.pl/ - niebezpiecznik.pl portal</p> <p>https://www.nist.gov/topics/cybersecurity - NIST cybersecurity knowledge base</p> <p>https://www.schneier.com/ - Bruce Schneier's blog</p> <p>https://www.cert.pl/ - CERT NASK PL</p> <p>https://www.enisa.europa.eu/ - ENISA portal</p>	
Example issues/ example questions/ tasks being completed	<ol style="list-style-type: none"> 1. Analyse an enterprise and its IT infrastructure and prepare the documentation. 2. Perform risk assessment of the analysed IT infrastructure. 3. Propose protection controls for the analysed IT infrastructure. 4. Present examples of critical infrastructures. 5. Present and discuss basic functions of firewalls. 		
Work placement	Not applicable		