GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Security of Computer Systems, PG_00047883						
Field of study	Informatics						
Date of commencement of studies	October 2020		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	Full-time studies		Mode of delivery		at the university		
Year of study	3		Language of instruction		Polish		
Semester of study	6		ECTS credits		4.0		
Learning profile	general academic profile		Assessment form		assessment		
Conducting unit	Department of Computer Architecture -> Faculty of Electronics, Telecommunications and Informatics						
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Piotr Rajchowski					
	Teachers	dr inż. Piotr Rajchowski					

Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	30.0	0.0	0.0	15.0	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	4.0	51.0	100

Subject objectives	The aim of the course is to familiarize the student with the risk and security policy of computer systems at the same time learning about common cryptographic algorithms and security access methods to databases.

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[K6_W03] Knows and understands, to an advanced extent, the construction and operating principles of components and systems related to the field of study, including theories, methods and complex relationships between them and selected specific issues - appropriate for the curriculum	The student has knowledge about using cryptographic protocols, and how to secure information systems with public access. Student has knowledge about commonly described attacks on information systems.	[SW2] Assessment of knowledge contained in presentation [SW1] Assessment of factual knowledge
	[K6_W04] Knows and understands, to an advanced extent, the principles, methods and techniques of programming and the principles of computer software development or programming devices or controllers using microprocessors or programmable elements or systems specific to the field of study, and organisation of systems using computers or such devices	The student has an ability of developing programs implementing the known cryptographic protocols and methods of database access. Student is able to describe and identify the way how to develop programs in the realities of the profession.	[SW3] Assessment of knowledge contained in written work and projects [SW2] Assessment of knowledge contained in presentation

Subject contents	Threats, risk, security policies. Security policy design and planning. Risk analysis and Disaster Recovery Plans. Personell security management. Phisical access control systems. Cryptographic techniques. Basic crytpographic algorithms. Cipher construction methods and modes of operation. One-way hash functions.. Authentication, identification, key exchange. Digital signature and PK certificates. Key management. Secure data transfer. Access control models. Operatin systems and application security. Advanced authentication symmetric, assymetric and hybrid protocols, identification and zero-knowledge protocols. Internet attacks. Socjal enginneering methods of system penetration. Development of web security. SSL/TSL protocol. Firewalls. PKMobile systems security. Security standards and directives. Security assessment of IT systems. Security audit.
Prerequisites and co-requisites	Basic programming skills and ability to work with databases

Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	colloqium (2)	50.0%	60.0%
	Project implementation	50.0%	40.0%

Recommended reading	Basic literature	1. Schneier, B., Applied Cryptography, 2nd ed. J.Wiley 1996. 2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone „Handbook of Applied Cryptography" 1997. 3. J. Stokłosa, T. Bilski, T. Pankowski – Data securty in IT systems, PWN 2001 (in Polish) 4. W. Stallings: Cryptography and Network. Security: Principles and Practice,. Prentice Hall, 1998 5. J. Pieprzyk, T. Hardjono, J. Seberry - Fundamentals of Computer Security, Springer, 2003. 6. R. Anderson - Security Engineering, Wiley 2008.
	Supplementary literature	1. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12 ,http://www.nist.org 2. S. Garfinkel. G. Spafford., Practical Unix and Iternet Security, O'Reilly, 1998, 2nd ed.
	eResources addresses	Uzupełniające Adresy na platformie eNauczanie: Bezpieczeństwo Systemów Komputerowych - 2023 - Moodle ID: 27747 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=27747

Example issues/ example questions/ tasks being completed	
Work placement	Not applicable