GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Information Security Management, PG_00038313		
Field of study	Automation, Robotics and Control Systems		
Date of commencement of studies	October 2022	Academic year of realisation of subject	2022/2023
Education level	second-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	1	Language of instruction	Polish
Semester of study	2	ECTS credits	2.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Control Engineering -> Faculty of Electrical and Control Engineering		
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Paweł Kowalski	
	Teachers	dr inż. Paweł Kowalski	

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	0.0	0.0	0.0	0.0	10.0	10

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	10	5.0	35.0	50

Subject objectives

Acquainting students with principles of information security management and methods of information security in computer systems and networks.

Learning outcomes

Course outcome	Subject outcome	Method of verification
K7_W07	The student has knowledge of information security management systems.	[SW1] Assessment of factual knowledge
K7_W09	The student can test the IT system in terms of security.	[SW3] Assessment of knowledge contained in written work and projects [SW2] Assessment of knowledge contained in presentation [SW1] Assessment of factual knowledge
K7_U08	The student has the necessary preparation to work in an industrial environment, conduct research, apply the principles of occupational health and safety.	[SU4] Assessment of ability to use methods and tools [SU5] Assessment of ability to present the results of task [SU1] Assessment of task fulfilment

Subject contents	Basic aspects of information security: identification, authenticity and authorization, confidentiality, integrity and accessibility. Hazards: users, attacks, malicious software, informatics wars. Types and methods of safety violation of computer systems. Methods and measures of information security. Methods and systems of the access control. Fire walls. Systems of intruders finding. Spam phenomenon and countermeasures. Virtual private networks: architectures and protocols. Cryptographic methods and algorithms. Basic principles of information security management. Identification of hazards, and analysis and assessment of risks. Basic strategies of information security management. A system of information security in company and institution. Requirements concerning the information security and protections with regard to standards: PN-ISO/ISO 17799, ISO/IEC TR 13335 and PN-ISO/IEC 27001:2007. Standard ISO/IEC 15408 and meaning of common criteria (CC). Life cycle and information security management. Basics of the protection system design with regard to technical and organizational aspects. Examples of solutions. The role of the board of directors. Audit of the information security management system. Methods and tools for the safety and security assessment. The quality and reliability management of software. Safety and security of wired and wireless networks. Safety of some protocols, hazards and countermeasures. Data coding mechanisms and authenticity. Electronic signature. Standards used in wireless networks and security mechanisms. Integrated functional safety and information security management in programmable industrial control and protection systems. Safety and security of distributed industrial computer networks.
Prerequisites and co-requisites	Knowledge concerning applications of the computer systems and networks, and programmable technologies in the industry. Basic knowledge about the identification of hazards, the reliability and safety analysis as well as the analysis and assessment of risks of technical plants and systems, including the critical infrastructure. Basic knowledge in the domain of cryptography.

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Technical paper	50.0%	50.0%
Presentation	50.0%	50.0%

Recommended reading

Basic literature

1. Anderson R.: Inżynieria zabezpieczeń. Wydawnictwo Naukowo Techniczne, Warszawa: 2005.
2. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwa Naukowo-Techniczne, Warszawa 2006.
3. Karpiński M. (red.): Bezpieczeństwo informacji. Wydawnictwo PAK, Warszawa 2012.
4. Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. Wydawnictwo Naukowe PWN, Warszawa 2008.
5. Liderman K.: Bezpieczeństwo informacyjne. Wydawnictwo Naukowe PWN, Warszawa 2012.
6. Schneier B.: Kryptografia dla praktyków. Wiley, PWN, 2002.
7. Wesołowski J., Namieśnik J.: Bezpieczeństwo i ochrona informacji. Politechnika Gdańska, Wydział Chemiczny, Gdańsk 2007.

Supplementary literature

1. Dostalek L.: Bezpieczeństwo protokołu TCP/IP. Wydawnictwo Naukowe PWN, Warszawa, 2003.
2. Kosmowski K.T.: Functional safety management in critical systems, Gdańsk, 2008.
3. Sankar K. i inni: CISCO. Bezpieczeństwo sieci bezprzewodowych. Wyd. Mikom, Warszawa, 2005.
4. PN-ISO/IEC 27001:2007: Technika informatyczna - Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania (Information technology Security techniquesInformation security management systemsRequirements).

eResources addresses

Adresy na platformie eNauczanie:

Example issues/ example questions/ tasks being completed

Information security related hazards.

Information security management system in a company.

Legal and standardization aspects of information security management.

Work placement	Not applicable