GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Introduction to cybersecurity, PG_00053947		
Field of study	Informatics		
Date of commencement of studies	October 2024	Academic year of realisation of subject	2025/2026
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	at the university
Year of study	2	Language of instruction	Polish
Semester of study	4	ECTS credits	2.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Computer Communications -> Faculty of Electronics, Telecommunications and Informatics		
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Wojciech Gumiński	
	Teachers	dr inż. Wojciech Gumiński	

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	15.0	0.0	0.0	15.0	0.0	30

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	30	2.0	18.0	50

Subject objectives

The aim of the course is learning cybersecurity basics. During classes students get to know selected security threats. A set of security functions is also presented: confidentiality, integrity and availability along with measures for achieving them. During project classes students practice cryptomaterial operations applied to basic, popular use cases.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K6_W44] knows and understands, to an advanced extent, architecture, design principles and methods of hardware and software support for local and distributed information systems, including computing systems, databases, computer networks and information applications, as well as the principles of human-computer interaction, the operation and evaluation criteria of data processing, storage and transfer methods, including computational algorithms, artificial intelligence and data mining as well as standards and methods of IT systems administration, monitoring of processes and robustness to undesirable phenomena and activities	Student lists and describes security attributes. Student lists the differences between symmetric and asymmetric cryptography algorithms and can provide examples of their applications.	[SW1] Assessment of factual knowledge
[K6_K03] is ready to meet social obligations, co-organise activities for the social environment, initiate actions for the public interest, think and act in an entrepreneurial way	Student is able to implement cryptographic information security.	[SK1] Assessment of group work skills [SK5] Assessment of ability to solve problems that arise in practice
[K6_U03] can design, according to required specifications, and make a simple device, facility, system or carry out a process, specific to the field of study, using suitable methods, techniques, tools and materials, following engineering standards and norms, applying technologies specific to the field of study and experience gained in the professional engineering environment	Student is able to apply presented security metrics. During project classes integrates/implements and presents their application in selected use case.	[SU5] Assessment of ability to present the results of task [SU1] Assessment of task fulfilment

Subject contents

Basic terms related to IT systems security, security functions: integrity, confidentiality, authentication. Classification of threats and attacks: information sniffing, modification, spoofing, targeted and non-targeted attacks, malware, botnets. Cryptography basics: symmetric and asymmetric cryptography, one time keys, block ciphers, stream ciphers, data integrity. Public key cryptography and PKI. Security in applications: PKI applications, operations of certificate-based solutions. Security management basics: security policy, security best practices, secure programming best practices.

Prerequisites and co-requisites

The ability to configure and operate popular operating systems

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Project	50.0%	50.0%
Lecture	50.0%	50.0%

Recommended reading

Basic literature	Lecture materials
Supplementary literature	Schneier B.: Kryptografia dla praktyków Bilski T., Pankowski T., Stokłosa J.: Bezpieczeństwo danych w systemach informatycznych Stallings W.: Cryptography and Network Security Gollmann D.: Computer security
eResources addresses	Adresy na platformie eNauczanie:

Example issues/ example questions/ tasks being completed

1. Deployment of selected cryptographic algorithms using popular frameworks
2. Application of PKI to mutual web server-client authentication
3. Application of PKI to e-mail signing and encryption

Work placement

Not applicable