GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Security of IT systems, PG_00071526						
Field of study	Technical Physics						
Date of commencement of studies	October 2023		Academic year of realisation of subject	2025/2026			
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	5.0			
Learning profile	general academic profile		Assessment form	exam			
Conducting unit	Division of Theoretical Physics and Quantum Informaton -> Institute of Physics and Applied Computer Science -> Faculty of Applied Physics and Mathematics -> Faculties of Gdańsk University of Technology						
Name and surname of lecturer (lecturers)	Subject supervisor		dr inż. Paweł Syty				
	Teachers		dr inż. Paweł Syty				
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	0.0	45.0	0.0	0.0	60
	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	60		5.0	60.0		125
Subject objectives	The aim of the course is to familiarise students with the basic concepts, threats and mechanisms of IT system protection in modern organisational environments. Students will gain knowledge in the field of data protection, network security, operating systems and applications, and will learn the principles of information security management. The course develops the ability to identify vulnerabilities, analyse risks and select appropriate security mechanisms in IT systems.						

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[K6_W02] Has systematized knowledge of the basics of physics, including mechanics, thermodynamics, electricity and magnetism, optics, atomic and particle physics, solid-state physics, nuclear and elementary particle physics.	Knows risk analysis methods, access control models and security architectures used in the design and operation of IT systems.	[SW1] Assessment of factual knowledge [SW3] Assessment of knowledge contained in written work and projects
	[K6_W05] Has knowledge of programming methodology and techniques, and the use of selected IT tools in physics and technology.	Has structured knowledge of the threats and vulnerabilities of IT systems, including the security of operating systems, computer networks, applications and cloud environments.	[SW1] Assessment of factual knowledge [SW3] Assessment of knowledge contained in written work and projects
	[K6_U07] Can present basic facts within the scope of physics and other scientific disciplines in a clear manner.	Can explain basic cybersecurity threats and the importance of protective mechanisms in an accessible manner to audiences with varying levels of technical knowledge.	[SU2] Assessment of ability to analyse information [SU5] Assessment of ability to present the results of task
	[K6_U08] Can prepare written works and speeches in Polish and English, concerning detailed issues of physics and related fields, and scientific disciplines.	Can prepare a report on the security analysis of an IT system and present its results in written and oral form, in Polish or English.	[SU3] Assessment of ability to use knowledge gained from the subject [SU5] Assessment of ability to present the results of task
	[K6_K01] Understands the need to learn and improve professional and personal competencies. Can inspire and organize other people’s learning process	Understands the importance of continuously updating knowledge in the field of cybersecurity in view of the rapidly changing nature of threats.	[SK5] Assessment of ability to solve problems that arise in practice [SK4] Assessment of communication skills, including language correctness

Subject contents	Course content – lecture 1. Introduction to IT system security Basic concepts: confidentiality, integrity, availability (CIA), vulnerability, threat, risk. Current trends in cybersecurity. 2. Security models and security policy Access control models (DAC, MAC, RBAC), security policy in an organisation. 3. Risk analysis in IT systems Identification of assets, threats and vulnerabilities. Qualitative and quantitative risk assessment methods. 4. IT system security architecture Security by Design and Security by Default, Zero Trust Model, Network Segmentation and Microsegmentation, Defence in Depth, Security Zones (DMZ), Attack Surface Modelling 5. Information security standards and norms Information Security Management System (ISMS), ISO/IEC 27000 family of standards, NIST Cybersecurity Framework 6. Operating system security Access control mechanisms, updates, system hardening, process isolation. 7. Computer network security Firewalls, IDS/IPS, network segmentation, VPN. 8. Web application security Common vulnerabilities (e.g. SQL injection, XSS), basics of secure programming. 9. Authentication and authorisation Password mechanisms, MFA, SSO, identity management. 10. Data security and privacy protection Data encryption at rest and in transit, backups, basics of legal regulations (e.g. GDPR). 11. Social engineering attacks and internal threats Phishing, spear phishing, social engineering, user awareness. 12. Security testing and auditing Penetration testing, vulnerability scanners, basics of security auditing. 13. Security incident management Incident response, forensics, business continuity plan (BCP). 14. Security in the cloud and distributed systems Service models (IaaS, PaaS, SaaS), threats and best practices. 15. Trends and challenges in cybersecurity AI in security, ransomware threats, IoT security. Course content – laboratory 1. Test environment and vulnerability analysis - Configuration of an isolated laboratory environment (e.g. virtual machines). - Basics of Linux/Windows system security. - Network scanning and service identification. - Detection of vulnerabilities in systems and applications. 2. System security monitoring and analysis - Event logging in operating systems - Log centralisation - Introduction to SIEM systems - Detection of anomalies in logs - Event correlation 3. Web application security - Identification of web application vulnerabilities. - Analysis of HTTP traffic. - Testing for SQL injection and XSS vulnerabilities. - Basics of secure web server configuration 4. Authentication and access control mechanisms - Password policy configuration. - Access control mechanisms in the operating system. - Firewall configuration. - Introduction to multi-factor authentication (MFA). 5. Incident response and post-breach analysis - Identification of security incidents. - Analysis of system logs. - Basics of digital forensics. - Preparation of incident reports.

<table>
<tr><td>Prerequisites and co-requisites</td><td></td></tr>
<tr><td>Assessment methods and criteria</td><td>
<table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td>oral assessment</td><td>50.0%</td><td>30.0%</td></tr>
<tr><td>performance of laboratory tasks</td><td>50.0%</td><td>50.0%</td></tr>
<tr><td>assessment of written work</td><td>50.0%</td><td>20.0%</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">Recommended reading</td><td>Basic literature</td><td>John Vacca, Computer and Information Security Handbook, Morgan Kaufmann, 2024
Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, Cengage Learning, 2021</td></tr>
<tr><td>Supplementary literature</td><td>Michael E. Whitman and Herbert J. Mattord, Management of Information Security, No Starch Press, 2019</td></tr>
<tr><td>eResources addresses</td><td></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td>Conducting a risk analysis for a sample IT system, identifying assets, threats and vulnerabilities.

Configuring basic operating system security mechanisms and assessing their effectiveness.

Performing a network scan and interpreting the results in the context of potential security vulnerabilities.</td></tr>
<tr><td>Practical activites within the subject</td><td>Not applicable</td></tr>
</table>

Document generated electronically. Does not require a seal or signature.