

Subject card

Subject name and code	Information Security (Classes), PG_00205615						
Field of study	National Security						
Date of commencement of studies	October 2027		Academic year of realisation of subject		2027/2028		
Education level	Bachelor's studies		Subject group		Obligatory subject group in the field of study Subject group related to practical vocational preparation		
Mode of study	full-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	practical		Assessment form		credit		
Conducting unit	Rada Uczelni						
Name and surname of lecturer (lecturers)	Subject supervisor		dr Konrad Ćwikliński				
	Teachers						
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	0.0	30.0	0.0	0.0	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		0.0		20.0	50
Subject objectives	<p>The objective of the course Information Security in the form of auditorium-based exercises is to prepare students to understand, analyze, and practically solve problems related to information security in the context of the functioning of the state, public institutions, and private entities.</p> <p>The course aims to develop the ability to identify information threats, assess risks, and apply countermeasures, including organizational, technical, and legal solutions. Particular emphasis is placed on building competencies in data protection, cybersecurity, incident management, and the analysis of modern hybrid and disinformation threats.</p> <p>As part of the exercises, students will become familiar with the practical aspects of information security from the basics of information analysis and source credibility assessment, through threat modeling, to the development of response procedures and securing information systems. The exercises include the analysis of real-world security breach cases, the creation of information security plans, as well as solving simulation-based and problem-oriented tasks.</p>						

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[BNL3_K04] Is prepared to be active in the labour market and is aware of the need to improve qualifications for responsible performance of professional roles.	Is prepared to work in the information protection sector and understands the need for continuous professional development.	[SK1] oral statement/conversation/discussion [SK2] presentation/project/paper/report
	[BNL3_U02] Analyses the causes and course of processes and their evolution relating to social, political, economic, legal, ethical and cultural aspects of security.	Analyzes the causes and effects of information threats in social, political, and legal contexts.	[SU1] oral statement/conversation/discussion [SU2] presentation/project/paper/report
	[BNL3_U05] Indicates and explains the role of a democratic state and civil society in the area of security.	Explains the role of democratic institutions in ensuring information security.	[SU1] oral statement/conversation/discussion [SU2] presentation/project/paper/report
	[BNL3_U07] Actively participates in socio-political life and attempts to participate in public discourse. Manages the self-education process, develops his work skills and new cognitive skills. Plans and organizes the work of oneself and the team, preparing social, political, economic and civic projects (including those involving cooperation with other people), using various sources and technological possibilities.	Participates in information security projects using digital sources and technological tools.	[SU1] oral statement/conversation/discussion [SU2] presentation/project/paper/report
	[BNL3_W13] Has knowledge of intellectual property law, including the protection of copyright and industrial property.	The student understands copyright and intellectual property protection principles in information systems.	[SW1] oral statement/conversation/discussion [SW2] presentation/project/paper/report
Subject contents	[BNL3_W08] At an advanced level, understands the mechanisms of risk management and decision-making in national security institutions.		
	Participates in information security projects using digital sources and technological tools.		
Subject contents	Course outline (auditory classes):		
	<ol style="list-style-type: none"> 1. Introduction. Basic concepts of information security. 2. Information classification. Protection of classified and sensitive data. 3. Sources and types of information threats. Examples of cyberattacks. 4. Risk analysis. Methods and risk assessment matrices. 5. Incident management. Response and reporting. 6. Information security policy. Document structure and creation. 7. Personal data protection. Copyright and IP law. 8. Information security audit principles and stages. 9. Audit tools. Checklists and documentation analysis. 10. ISMS systems. ISO/IEC 27001 standard. 11. Social engineering. Human factor in threats. 12. Cybersecurity vs. information security. 13. Ethics and responsibility. Whistleblowing. 14. Audit project team work. 15. Project presentations.. Summary. 		
Prerequisites and co-requisites			
Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	collaboration	50.0%	35.0%
	Participation in class activities	50.0%	65.0%
Recommended reading	Basic literature		
	<ol style="list-style-type: none"> 1. Solms R. von, van Niekerk J., Information Security Context and Techniques, Routledge, London, 2017. 2. Harris S., CISSP All-in-One Exam Guide, McGraw-Hill, New York, 2022. 3. Smith R.E., Elementary Information Security, Jones & Bartlett Learning, Burlington, 2021. 4. ISO/IEC 27001:2022 Information Security Management Systems Requirements, ISO, Geneva, 2022. 5. Peltier T.R., Information Security Policies, Procedures, and Standards, Auerbach Publications, Boca Raton, 2021. 		

	Supplementary literature	<ol style="list-style-type: none"> 1. Tipton H.F., Krause M., Information Security Management Handbook, Auerbach Publications, Boca Raton, 2021. 2. Andress J., The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress, Oxford, 2020. 3. Greengard S., Cybersecurity and Privacy: Issues in the Age of Digital Transformation, MIT Press, Cambridge, 2021. 4. NIST SP 800-30, Guide for Conducting Risk Assessments, National Institute of Standards and Technology, Gaithersburg, 2012. 5. Białek R., Bezpieczeństwo informacji w systemach informatycznych, PWN, Warszawa, 2018. 6. Disterer G., ISO/IEC 27000, 27001 and 27002 for Information Security Management, Journal of Information Security, 2013.
	eResources addresses	
Example issues/ example questions/ tasks being completed	<ol style="list-style-type: none"> 1. Develop an information security policy for a small company. 2. Prepare a risk assessment for a selected IT system. 3. Identify weak points in an organizations information security. 4. Conduct a security audit of documentation in a fictional institution. 5. Write a report after analyzing a personal data breach incident. 	
Work placement	Not applicable	

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