University of Gdańsk

Subject card

Subject name and code	Information Security (Lecture), PG_00205429		
Field of study	National Security		
Date of commencement of studies	October 2026	Academic year of realisation of subject	2026/2027
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	1.0
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	15.0	0.0	0.0	0.0	0.0	15

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	15	0.0	10.0	25

Subject objectives

The aim of the course 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. The course is designed to develop the ability to identify information threats, assess risks, and apply appropriate countermeasures, including organizational, technical, and legal tools.

Particular emphasis is placed on building competencies in data protection, cybersecurity, incident management, and the analysis of contemporary hybrid and disinformation threats. During the exercises, students will gain practical knowledge of information security from information analysis and source credibility assessment, through threat modeling, to the development of response procedures and the protection of information systems.

The course includes the analysis of real-world security breaches, the creation of information security plans, and the resolution of simulation and problem-based tasks.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[BNL3_W08] At an advanced level, understands the mechanisms of risk management and decision-making in national security institutions.	Has an advanced understanding of mechanisms and is able to identify them in risk management and decision-making in national security institutions.	[SW1] oral statement/ conversation/discussion [SW2] presentation/project/paper/ report [SW5] implementation of a problem task
[BNL3_W11] Has advanced knowledge about security strategies at the provincial and national levels.	Has advanced knowledge of security strategies at the regional and national levels.	[SW1] oral statement/ conversation/discussion [SW2] presentation/project/paper/ report [SW5] implementation of a problem task
[BNL3_W13] Has knowledge of intellectual property law, including the protection of copyright and industrial property.	Knows and understands the principles of intellectual property law. Has knowledge in the field of copyright and industrial property protection.	[SW1] oral statement/ conversation/discussion [SW2] presentation/project/paper/ report [SW5] implementation of a problem task
[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 for activity on the labor market, aware of the need to improve qualifications and to perform professional roles responsibly.	[SK1] oral statement/conversation/ discussion [SK5] implementation of a problem task [SK8] observation of student's independent or team work
[BNL3_U05] Indicates and explains the role of a democratic state and civil society in the area of security.	Identifies and explains the role of a democratic state and civil society in the area of security	[SU1] oral statement/conversation/ discussion [SU5] implementation of a problem task [SU8] observation of student's independent or team work
[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.	Actively participates in socio-political life and engages in public discourse. Plans and organizes own and team work, preparing social, political, economic, and civic projects using various sources and technologies.	[SU1] oral statement/conversation/ discussion [SU5] implementation of a problem task [SU8] observation of student's independent or team work
[BNL3_U06] Is able to analyse the causes and effects of security threats and indicates countermeasures. Plans own and team's work in the field of threat analysis and risk assessment.	Is able to analyze the causes and consequences of security threats and indicates countermeasures. Plans own and team work in the field of threat analysis and risk assessment.	[SU1] oral statement/conversation/ discussion [SU5] implementation of a problem task [SU8] observation of student's independent or team work

Subject contents	Course Outline: Information Security (lecture) 1. Introduction to Information Security • Key definitions: information, security, data, knowledge • The distinction between information security and cybersecurity • The role of information security in national and international security systems 2. 3. Information as a Strategic Resource • The significance of information in the network and information society • Information as a tool of power, influence, and control • Information management models and strategies 4. 5. Legal Foundations of Information Security • National legislation (e.g., GDPR, the Act on the Protection of Classified Information) • International and EU regulations (e.g., GDPR, NIS2) • Institutional and individual responsibility 6. 7. Information Threats Typologies and Classifications • Disinformation, propaganda, fake news, media manipulation • Cyberattacks, data breaches, digital espionage • Psychological and sociological aspects of information threats 8. Critical Infrastructure and Information Security • What is information-critical infrastructure • The impact of IT system failures on the functioning of the state and society • Models of securing information infrastructure 9. Institutions Responsible for Information Security • The role of the state, intelligence services, military, public administration • CERT, CSIRT, ABW, NASK structures and competencies • International and interagency cooperation 10. Personal Data Protection and Privacy • The concept of privacy and personal data in the digital age • Basic principles of data protection (GDPR) • Best practices for secure data processing and storage 11. Cybersecurity as a Component of Information Security • Cyberspace and cyber threats • DDoS attacks, phishing, ransomware examples and mechanisms • Cybersecurity policies 12. Information Warfare and Influence Operations • The concept of information warfare historical and contemporary aspects • Psychological operations (PSYOPS), narratives, and memetics • Case studies: Russia, China, the Middle East, NATO 13. Media, Journalism, and Information Security • Media ethics and journalistic responsibility • Manipulation of information in traditional and social media • Algorithms, information bubbles, and radicalization 14. Artificial Intelligence and Information • The role of AI in information management and analysis • Deepfakes, generative AI, bots, and their role in disinformation • Ethical and technological challenges 15. State Information Policy • Examples of information policies in selected countries • Strategic information management during crises and conflicts • The role of spokespersons, official channels, and crisis communication 16. Education and Public Information Awareness • Media literacy, digital hygiene, information culture • Educational programs in schools and universities • Societal resilience to manipulation 17. Case Studies Analysis • Case studies: information attacks, data breaches, influence operations • Discussion and analysis of failures, strategies, and consequences • Conclusions and best practices 18. Summary and Final Assessment Preparation • Review of key concepts and topics • Q&A session • Consultations and final remarks

Prerequisites and co-requisites	Prerequisites: Scope of Knowledge, Skills, and Competences 1. Required knowledge and skills prior to the course: Before commencing the lecture course Information Security, students should possess: • Basic knowledge in the field of social and political sciences, particularly concerning the functioning of the state, public institutions, principles of democracy, and governance. • General understanding of national and international security issues, including familiarity with fundamental concepts such as internal security, asymmetric threats, and cybersecurity. • Ability to think critically and analyze academic texts, as well as interpret data and information from various sources. • Intermediate-level digital competencies, enabling effective use of the Internet, basic IT tools, and online educational platforms (e.g., Moodle, MS Teams, eUczelnia). • Foundations of law, especially constitutional law, as well as basic knowledge of data protection regulations and access to public information. 2. Required completion of other courses (if applicable): It is recommended that students have previously completed at least one of the following courses (or their equivalents in the study program): • Introduction to National or Internal Security, • Foundations of the State and Law, • Basics of Political Science, • Introduction to Information Systems in Public Administration, • Cybersecurity Fundamentals (if offered earlier in the curriculum).
Assessment methods and criteria	

Subject passing criteria	Passing threshold	Percentage of the final grade
Activity during lectures and individual work (e.g. case study analysis, participation in discussions)	50.0%	50.0%
Participation in lectures and independent student work (e.g., case analysis, class discussions)	50.0%	50.0%

Recommended reading	Basic literature	Literatura podstawowa (publikacje polskojęzyczne) 1. Olejnik, S., Bezpieczeństwo informacyjne państwa, Wydawnictwo Naukowe PWN, Warszawa, 2022. 2. Wojciechowski, S., Bezpieczeństwo informacyjne w stosunkach międzynarodowych, Difin, Warszawa, 2020. 3. Kulesza, J., Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer, Warszawa, 2021. 4. Cieślak, M., Dezinformacja jako zagrożenie dla bezpieczeństwa państwa, Wydawnictwo Naukowe Uniwersytetu Wrocławskiego, Wrocław, 2021. 5. Piechowiak-Lamparska, J., Wojna informacyjna: teoria i praktyka, Uniwersytet Mikołaja Kopernika, Toruń, 2020. 6. Banasik, M., Wojna informacyjna i wojna poznawcza, Wydawnictwo Difin, Warszawa, 2023. Literatura podstawowa (publikacje anglojęzyczne) 1. Castells, M., The Rise of the Network Society (The Information Age: Economy, Society and Culture, Vol. 1), Wiley-Blackwell, Oxford, 2010. 2. Rid, T., Active Measures: The Secret History of Disinformation and Political Warfare, Farrar, Straus and Giroux, New York, 2020. 3. Singer, P.W., Brooking, E.T., LikeWar: The Weaponization of Social Media, Houghton Mifflin Harcourt, Boston, 2018. 4. Kello, L., The Virtual Weapon and International Order, Yale University Press, New Haven, 2017. 5. Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, New York, 2019. 6. Nye, J.S., Soft Power: The Means to Success in World Politics, PublicAffairs, New York, 2004. 7. Geers, K. (ed.), Strategic Cyber Security, NATO CCD COE Publications, Tallinn, 2011.

	Supplementary literature	Literatura uzupełniająca (polskojęzyczna) 1. Marciniak, T., Cyberterroryzm i cyberwojna we współczesnym świecie, Difin, Warszawa, 2020. 2. Kozłowski, A., Bezpieczeństwo cyfrowe państwa, Wydawnictwo Naukowe UAM, Poznań, 2019. 3. Piech, K., Zarządzanie informacją w administracji publicznej, CeDeWu, Warszawa, 2018. 4. Świderska, M., Dezinformacja jako narzędzie walki politycznej, ASPRA-JR, Warszawa, 2016. 5. Szubrycht, T. (red.), Bezpieczeństwo informacyjne. Konteksty teorii i praktyki, Wydawnictwo WAT, Warszawa, 2021. Literatura uzupełniająca (anglojęzyczna) 1. Newman, N., Fletcher, R., Kalogeropoulos, A., Reuters Institute Digital News Report 2024, Reuters Institute, Oxford, 2024. 2. Lin, H., Cybersecurity Ethics, Oxford University Press, Oxford, 2021. 3. Moore, M., Tambini, D. (eds.), Digital Dominance: The Power of Google, Amazon, Facebook, and Apple, Oxford University Press, Oxford, 2018. 4. Paul, C., Information Operations Doctrine and Practice: A Reference Handbook, Praeger, Santa Barbara, 2008. 5. West, D.M., The Future of Work: Robots, AI, and Automation, Brookings Institution Press, Washington D.C., 2018.
	eResources addresses	

Example issues/ example questions/ tasks being completed	Sample discussion or exam topics: 1. Differences between information security and cybersecurity. 2. Information as a tool of power and control analysis of contemporary examples. 3. Disinformation and fake news as threats to national security. 4. Structure and competencies of institutions responsible for information security in Poland. 5. The impact of artificial intelligence and deepfakes on information manipulation. 6. The role of the information society in enhancing resilience to information threats. 7. Legal foundations of personal data protection comparison of Polish RODO and EU GDPR. 8. Information warfare strategies used by Russia and China. 9. Ethical challenges related to the use of data in politics and marketing. 10. State information policy during crises and armed conflicts. Sample test or exam questions: 1. Explain the concept of strategic information and provide an example of its application. 2. List and describe three main types of information threats. 3. What are the key principles of personal data processing according to GDPR? 4. How do influence operations work in the context of social media? 5. Characterize the role of CERT and CSIRT institutions in the information security system. 6. How do social media contribute to social polarization and information insecurity? 7. What information protection measures are used by public administration? 8. What is infodemic and what are its consequences? Sample practical assignments (for advanced or optional 1. Case study analysis Analyze a real-world data breach in a public institution and identify failures in information security management. 2. Critical media content analysis Identify manipulation and disinformation elements in a news article or social media post. 3. Information threat mapping Prepare a map of the most common information threats in public administration or the healthcare sector. 4. Academic debate Does artificial intelligence threaten individual information freedom? Prepare arguments for and against. 5. Crisis communication simulation Prepare and present a press release from a public institution following a cyberattack.
Work placement	Not applicable

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