University of Gdańsk

Subject card

Subject name and code	National Cybersecurity System, PG_00179304		
Field of study	National Security		
Date of commencement of studies	October 2024	Academic year of realisation of subject	2024/2025
Education level	Master's studies	Subject group	Obligatory subject group in the field of study Humanistic-social subject group
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	Faculty of Social Sciences -> Rector		
Name and surname of lecturer (lecturers)	Subject supervisor	dr Piotr Robakowski	
	Teachers	dr Piotr Robakowski	

Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	30.0	0.0	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	30.0	60

Subject objectives	The objective of the course "National Cybersecurity System" is to provide students with comprehensive knowledge about the structure, principles, and procedures related to ensuring cybersecurity in Poland, in accordance with the NIS Directive (Network and Information Systems) and the national Cybersecurity Act. The course covers the analysis of cyber threats, risk management mechanisms, and the roles and responsibilities of key institutions and entities responsible for protecting critical infrastructure.

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[BNMU2_U14] Has in-depth skills in searching and selecting sources and has extensive knowledge of technological possibilities for searching information, which uses for further development.	He possesses advanced skills in searching for and selecting legal sources in the field of IT security and has extensive knowledge of technological capabilities used to seek information on data protection methods.	[SU4] test/exam - oral or written
	[BNMU2_K01] Is prepared to be active in the labour market in the area of security, is aware of the need to independently improve qualifications, collect and analyse information, critically assesses the knowledge possesses and acquires.	He is prepared for activities in the IT security job market, understands the necessity of continuously improving his qualifications, and is capable of gathering and analyzing information in the field of cyberspace impact.	[SK1] oral statement/conversation/ discussion
	[BNMU2_W11] Has in-depth knowledge of security strategies at provincial and national levels.	He has advanced knowledge of cybersecurity strategies	[SW4] test/exam - oral or written
	[BNMU2_W09] Has an in-depth and structured knowledge of the essence, dynamics, and specificity of security threats in various spheres of social life.	He has advanced and organized knowledge about the nature, dynamics, and specifics of cybersecurity threats in various areas of social life.	[SW4] test/exam - oral or written
	[BNMU2_U03] Analyses in-depth the causes and course of processes and their evolution related to security, predicts challenges, trends and threats to the social, political, legal, economic and ethical environment using tools and methods specific to security sciences.	He deeply analyzes the causes and progression of processes and their evolution related to cybersecurity, forecasting challenges, trends, and threats to the social, political, legal, economic, and ethical aspects of cyberspace impact.	[SU1] oral statement/conversation/ discussion

Subject contents	**Introduction to Cybersecurity** • Definition of cybersecurity • Importance of cybersecurity in national and global contexts • Basic concepts and terms related to cybersecurity **2. Legal Framework of Cybersecurity** • NIS Directive (Network and Information Systems Directive) • National Cybersecurity System Act • Other national and international cybersecurity regulations **3. Structure of the National Cybersecurity System** • Organization and role of key institutions (e.g., CERT Polska, ABW, NASK) • Mechanisms for intersectoral cooperation • Roles and responsibilities of public administration, the private sector, and citizens **4. Identification and Analysis of Cyber Threats** • Types of threats (e.g., malware, phishing, ransomware) • Techniques and methods used by cybercriminals • Case studies of cyberattacks and their consequences **5. Risk Assessment and Risk Management** • Methods of risk assessment in cybersecurity • Risk management: identification, analysis, control • Implementation of risk management strategies in organizations **6. Protection of Critical Infrastructure** • Definition and importance of critical infrastructure • Methods for protecting critical infrastructure from cyberattacks • International cooperation in critical infrastructure protection **7. Cybersecurity Technologies and Tools** • Overview of the latest cybersecurity technologies and tools • Intrusion Detection and Prevention Systems (IDS/IPS) • Firewalls, antivirus software, encryption **8. Incident Response Planning and Management** • Creating and implementing incident response plans • Incident management process: identification, response, recovery • Cyber incident exercises and simulations **9. Cybersecurity Education and Awareness** • Educational programs and cybersecurity training • Raising awareness among users and employees • Best practices and case studies **10. Future of Cybersecurity** • Trends and future challenges in cybersecurity • Role of artificial intelligence and machine learning in cybersecurity • Future legislative changes and their impact on cybersecurity
Prerequisites and co-requisites	

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
	60.0%	20.0%
	60.0%	80.0%

Recommended reading

Basic literature

- **Michael N. Schmitt**, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", Cambridge University Press, 2017.
- **NIS Directive (EU) 2016/1148**, "Official Journal of the European Union", 2016.
- **Ustawa o krajowym systemie cyberbezpieczeństwa**, "Dziennik Ustaw Rzeczypospolitej Polskiej", 2018.
- **Kimberly Kagan**, "Cybersecurity in Our Digital Lives", Springer, 2021.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

	Supplementary literature	• **Andrew Hoffman**, "Web Application Security: Exploitation and Countermeasures for Modern Web Applications", O'Reilly Media, 2020. • **D. Ben H. Thacker, G. Mark Hardy**, "Building a Cyber Resilient Business", Artech House, 2019. • **Jason Andress, Steve Winterfeld**, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", Syngress, 2020. • **Raef Meeuwisse**, "Cybersecurity for Beginners", Cyber Simplicity Ltd, 2019.
	eResources addresses	
Example issues/ example questions/ tasks being completed	**Legal Framework of Cybersecurity:** • Describe the main provisions of the NIS Directive (Network and Information Systems Directive) and their significance for the national cybersecurity system. • Explain the key assumptions of the National Cybersecurity System Act and discuss its impact on the public and private sectors. **2. Structure of the National Cybersecurity System:** • Present the organizational structure of the national cybersecurity system, highlighting key institutions and their roles. • Discuss the mechanisms of intersectoral cooperation in cybersecurity. **3. Identification and Analysis of Cyber Threats:** • Characterize different types of cyber threats such as malware, phishing, and ransomware, and their potential impacts. • Analyze examples of real-world cyberattacks, discussing their course and consequences. **4. Risk Assessment and Risk Management:** • Explain the methods of risk assessment in cybersecurity and discuss the process of risk management. • Describe the steps involved in implementing risk management strategies in organizations. **5. Protection of Critical Infrastructure:** • Define the concept of critical infrastructure and explain its importance in the context of cybersecurity. • Discuss methods for protecting critical infrastructure from cyberattacks and provide examples of best practices. **6. Cybersecurity Technologies and Tools:** • Provide an overview of the latest technologies and tools used to ensure cybersecurity, such as Intrusion Detection and Prevention Systems (IDS/IPS). • Discuss the role of firewalls, antivirus software, and encryption in data protection. **7. Incident Response Planning and Management:** • Describe the process of creating and implementing incident response plans. • Discuss the stages of incident management, including identification, response, and recovery. **8. Cybersecurity Education and Awareness:** • Explain the importance of education and training in cybersecurity for employees and users. • Discuss best practices in raising awareness about cyber threats. **9. International Aspects of Cybersecurity:** • Explain the principles of transferring personal data to third countries in accordance with GDPR and the NIS Directive. • Discuss the role of international cooperation in protecting cyberspace. **10. Future of Cybersecurity:** - Analyze future trends and challenges in cybersecurity, including the role of artificial intelligence and machine learning. - Present anticipated legislative changes and their potential impact on cybersecurity.	
Work placement	Conducted during student internships in public administration institutions.	

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