University of Gdańsk

Subject card

Subject name and code	Cybersecurity - lecture, PG_00134172						
Field of study	Criminology						
Date of commencement of studies	October 2024		Academic year of realisation of subject	2026/2027			
Education level	Bachelor's studies		Subject group	Obligatory subject group in the field of study			
Mode of study	part-time studies		Mode of delivery	at the university			
Year of study	3		Language of instruction	Polish			
Semester of study	6		ECTS credits	2.0			
Learning profile	academic		Assessment form				
Conducting unit	Department of Legal Informatics -> Faculty of Law and Administration -> Rector						
Name and surname of lecturer (lecturers)	Subject supervisor		mgr Patryk Ciurak				
	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		35.0	50
Subject objectives	The aim of the course is: to present the knowledge and skills necessary to develop cyber risk mitigation projects and strategies, including the appropriate legal steps to take in response to cyber attacks; to develop the knowledge and skills necessary to develop cyber risk mitigation projects and strategies, including the appropriate legal steps to take in response to cyber attacks, to learn the role and importance of a risk-based approach to cyber security across the organisation.						

Learning outcomes

Course outcome	Subject outcome	Method of verification
[KRYML3_UW01] The graduate can observe and interpret social phenomena, analyzes their relations with various areas of criminology.	The student: 1. knows the basic ways to prevent attacks on information systems, combat such attacks, secure evidence and report security incidents. 2. is able to perform a risk analysis of a system, workstation, organisation and process. 3. is able to analyse and understand information related to the responsibilities of the main actors in the field of cyber security. 4. is able to apply in practice the mechanisms of the national cyber security system.	[SU3] text preparation/written work [SU4] test/exam - oral or written [SU5] implementation of a problem task
[KRYML3_UU02] He/she can use basic theoretical knowledge in the field of criminology and related disciplines in order to analyze, interpret and solve problems related to criminology.	Student. 1. knows the responsibilities and powers of state and private entities resulting from the use of new information and communication technologies. 2. knows what actions should be taken to limit threats from cyberspace.	[SU3] text preparation/written work [SU4] test/exam - oral or written [SU5] implementation of a problem task
[KRYML3_KK01] The graduate is aware of the level of his/her knowledge and skills and understands the need for lifelong learning.	The student: 1. maintains the basic principles of cyber hygiene in the work and home environment. 2. is able to provide advice on information security issues. 3. understands the complex interdisciplinary relationships involved in the functioning of the national cyber security system.	[SK3] text preparation/written work [SK4] test/exam - oral or written [SK5] implementation of a problem task

Subject contents

1. Basic concepts related to cyber security.
2. Cyberspace and the Internet
3. Legal models for regulating cyberspace
4. Regulation of the Internet
5. Computer networks and basic categories of cybercrimes
6. The EU cyber security regime. Legal framework
7. Cyber hygiene

Prerequisites and co-requisites

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Written solution to a problem issue	51.0%	100.0%

Recommended reading

Basic literature

C. Banasiński, Cyberbezpieczeństwo. Zarys wykładu, wyd. 2. Wolters Kluwer, Warszawa 2023

K. Czaplicki, A. Gryszczyńska, G. Szpor [red.:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer, Warszawa 2019

Supplementary literature

1. *F. Wołowski, J. Zawiła-Niedźwiecki,* Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków 2012;
2. *J. Łuczak, M. Tyburski,* Systemowe zarządzanie bezpieczestwem informacji wg ISO/IEC 27001:2005, Wyd. UE, Poznań 2009;
3. *K. Liderman,* Bezpieczeństwo informacyjne : nowe wyzwania, Warszawa, 2017
4. *D. Szostek* [red.:] Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej/adwokackiej/notarialnej/ komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej C.H.Beck, Warszawa 2018;
5. *D. Lisiak-Felicka, M. Szmit,* Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, European Association For Security, Kraków 2016, https://www.researchgate.net/publication/301204372_Cyberbezpieczenstwo_administracji_publicznej_w_Pols link/570c7d4d08ae2eb94223c4f7/download
6. *M. Szmit,* Wybrane zagadnienia opiniowania sądowo-informatycznego, European Association For Security, Kraków 2014;
7. *N. Polemi,* Port Cybersecurity. Securing critical information ifrastructures and supply chains, Elsevier, Amsterdam-Oksford-Cambridge 2018;
8. *J. Kossoff,* Cybersecurity Law, Wiley, Hoboken 2020.

eResources addresses

Example issues/ example questions/ tasks being completed	
Work placement	Not applicable

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