University of Gdańsk

Subject card

Subject name and code	Cybersecurity - lecture, PG_00131767		
Field of study	Criminology		
Date of commencement of studies	October 2026	Academic year of realisation of subject	2028/2029
Education level	Bachelor's studies	Subject group	Obligatory subject group in the field of study 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	2.0
Learning profile	academic	Assessment form	exam
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	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	20.0	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_W04] Has advanced knowledge and understands the legal and institutional conditions of the functioning of state authorities, as well as the role of these authorities in counteracting pathological phenomena, especially crimes; also knows the internal structure of these authorities and their competences.	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.	[SW4] test/exam - oral or written [SW3] text preparation/written work [SW5] implementation of a problem task
[KRYML3_W03] Has advanced knowledge and understands the relationships and social and psychological determinants between selected phenomena related to criminal acts, including key social and psychological phenomena relevant to the context of the studied field.	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.	[SW4] test/exam - oral or written [SW3] text preparation/written work [SW5] implementation of a problem task

<table>
<tr><td>Subject contents</td><td colspan="3">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</td></tr>
<tr><td>Prerequisites and co-requisites</td><td colspan="3"></td></tr>
<tr><td>Assessment methods and criteria</td><td colspan="3"><table><tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr><tr><td>Written solution to a problem issue</td><td>51.0%</td><td>100.0%</td></tr></table></td></tr>
<tr><td rowspan="3">Recommended reading</td><td>Basic literature</td><td colspan="2">1. C. Banasiński, Cyberbezpieczeństwo. Zarys wykładu, wyd. 2. Wolters Kluwer, Warszawa 2023
2. K. Czaplicki, A. Gryszczyńska, G. Szpor [red.:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer, Warszawa 2019</td></tr>
<tr><td>Supplementary literature</td><td colspan="2">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 bezpieczeństwem 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_Polsce_' 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.</td></tr>
<tr><td>eResources addresses</td><td colspan="2"></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td colspan="3"></td></tr>
<tr><td>Work placement</td><td colspan="3">Not applicable</td></tr>
</table>

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