University of Gdańsk

Subject card

Subject name and code	Cybercrime and cybersecurity - auditorium classes, PG_00132526		
Field of study	Criminology		
Date of commencement of studies	October 2024	Academic year of realisation of subject	2025/2026
Education level	Master'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	2	Language of instruction	Polish
Semester of study	3	ECTS credits	1.0
Learning profile	academic	Assessment form	credit
Conducting unit	Department of Legal Informatics -> Faculty of Law and Administration -> Rector		
Name and surname of lecturer (lecturers)	Subject supervisor	mgr Patryk Ciurak	
	Teachers	mgr Patryk Ciurak	

Lesson types

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	0.0	10.0	0.0	0.0	0.0	10

E-learning hours included: 0.0

eNauczanie source addresses:
Moodle ID: 12526 Cyberprzestępczość i cyberbezpieczeństwo (Kryminologia)
https://mdl.ug.edu.pl/course/view.php?id=12526

Additional information:

Discussion
Case studies
Work in groups

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	10	0.0	15.0	25

Subject objectives

Students learn about the legal, procedural and technical aspects of information technology crimes and become familiar with the basic principles and mechanisms of information systems security, as well as the legal norms governing the use of computers etc. and ICT networks.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[KRYMMU2_KK01] The graduate is aware of the level of his/her knowledge and skills, and also understands the need of lifelong learning	The student does not abuse information systems by violating other people's privacy, do not commit criminal or unethical acts related to the use of computers and information networks, do not use software to which they have not acquired rights.	[SK1] oral statement/conversation/ discussion [SK4] test/exam - oral or written [SK5] implementation of a problem task [SK8] observation of student's independent or team work
[KRYMMU2_WG01] The graduate demonstrates widened knowledge about legal science and related penal sciences, their the place in the system of sciences and mutual relation	The student is familiar with the dangers of using computers and IT networks, the principles of IT systems security management, the dangers of loss of privacy, the principles of intellectual property protection and the basics of patent and copyright law.	[SW4] test/exam - oral or written [SW1] oral statement/ conversation/discussion [SW5] implementation of a problem task
[KRYMMU2_WG04] The graduate demonstrates widened knowledge about various types of crime and the ways of preventing crime	The student is familiar with the dangers of using computers and IT networks, the principles of IT systems security management, the dangers of loss of privacy, the principles of intellectual property protection and the basics of patent and copyright law.	[SW4] test/exam - oral or written [SW1] oral statement/ conversation/discussion [SW5] implementation of a problem task
[KRYMMU2_KR05] The graduate is ready to prepare and participate in the preparation of social projects taking into consideration legal, economic and political aspects, including the preparation and implementation of projects co-financed by the European Union’s funds	The student does not abuse information systems by violating other people's privacy, do not commit criminal or unethical acts related to the use of computers and information networks, do not use software to which they have not acquired rights.	[SK1] oral statement/conversation/ discussion [SK4] test/exam - oral or written [SK5] implementation of a problem task [SK8] observation of student's independent or team work
[KRYMMU2_UW04] He/she can apply legal and professional principles and norms in taking up the activity of criminologist	The student is able to find information from literature, the Internet and other sources in the field of information systems security, interpret the aforementioned information, draw conclusions and formulate and justify opinions, prepare security policy for the organisation.	[SU1] oral statement/conversation/ discussion [SU4] test/exam - oral or written [SU5] implementation of a problem task [SU8] observation of student's independent or team work
[KRYMMU2_KR08] He/ she is aware of the level of own knowledge and skills, and understands the need for lifelong learning	The student does not abuse information systems by violating other people's privacy, do not commit criminal or unethical acts related to the use of computers and information networks, do not use software to which they have not acquired rights.	[SK1] oral statement/conversation/ discussion [SK4] test/exam - oral or written [SK5] implementation of a problem task [SK8] observation of student's independent or team work
[KRYMMU2_UW05] He/she is able to assess the usefulness of typical procedures and good practice to carry out tasks connected with various spheres of criminology	The student is able to find information from literature, the Internet and other sources in the field of information systems security, interpret the aforementioned information, draw conclusions and formulate and justify opinions, prepare security policy for the organisation.	[SU1] oral statement/conversation/ discussion [SU4] test/exam - oral or written [SU5] implementation of a problem task [SU8] observation of student's independent or team work
[KRYMMU2_UK02] He/she is prepared for active participation in groups, organizations and institutions connected with the problem of crime and other related phenomena. He/she is also able to communicate with specialists and non-specialists in criminology	The student is able to find information from literature, the Internet and other sources in the field of information systems security, interpret the aforementioned information, draw conclusions and formulate and justify opinions, prepare security policy for the organisation.	[SK1] oral statement/conversation/ discussion [SK4] test/exam - oral or written [SK5] implementation of a problem task [SK8] observation of student's independent or team work
[KRYMMU2_UW01] The graduate utilizes theoretical knowledge in the field of criminology and the related scientific disciplines to analyze and interpret problems connected with widely understood crime	The student is able to find information from literature, the Internet and other sources in the field of information systems security, interpret the aforementioned information, draw conclusions and formulate and justify opinions, prepare security policy for the organisation.	[SU1] oral statement/conversation/ discussion [SU4] test/exam - oral or written [SU5] implementation of a problem task [SU8] observation of student's independent or team work

Course outcome	Subject outcome	Method of verification
[KRYMMU2_UW02] He/she acquires knowledge independently and develops his/her professional skills using various sources (in native and foreign language) and modern technologies	The student is able to find information from literature, the Internet and other sources in the field of information systems security, interpret the aforementioned information, draw conclusions and formulate and justify opinions, prepare security policy for the organisation.	[SU1] oral statement/conversation/ discussion [SU4] test/exam - oral or written [SU5] implementation of a problem task [SU8] observation of student's independent or team work

Subject contents

Cyber-hygiene and accountability of online activities
Identity theft
Spoofing
Phishing
Man-in-the-Middle
HTML/SQL Injection, formjacking
Botnet, DDoS
Disinformation, Fake News
Social engineering
OSINT
Risk analysis

Prerequisites and co-requisites

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Test	51.0%	100.0%

Recommended reading

Basic literature	J. Kosiński, Paradygmaty cyberprzestępczości, Difin, Warszawa 2015 C.Banasiński, M.Rojszczak, Cyberbezpieczeństwo wyd. 2, WoltersKluwer, Warszawa 2023 Wprowadzenie do bezpieczeństwa IT, t. 1, red. M. Sajdak, Securitum (Kraków) 2024 Wprowadzenie do bezpieczeństwa IT, t. 2, red. M. Sajdak, Securitum (Kraków) 2025
Supplementary literature	F.Wołowski, J.Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych, edu-Libri, Warszawa 2012 K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2022 M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securitum 2023 D.Lisiak-Felicka, M.Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, IASF, Kraków 2016, ss. 222; https://www.netcomplex.pl/blog/wp-content/uploads/2016/04/Cyberbezpieczenstwo_Lisiak_Felicka__Szmit.pdf D.Siemieniecka, M.Skibińska, K.Majewska, Cyberagresja zjawisko, skutki, zapobieganie, UMK 2020, ss. 198; https://wydawnictwo.umk.pl/pl/products/5275/cyberagresja-zjawisko-skutki-zapobieganie M.Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, Wyd. II, PTI, Warszawa 2014; ss. 238; https://historiainformatyki.pl/historia/dokument.php?nonav=&nrar=6&nrzesp=6&sygn=V%2F1%2F7&handle=1&folder=1 J.Wasilewski, Cyberprzestępczość wybrane aspekty prawnokarne oraz kryminalistyczne, Uniw. w Białymstoku, Białystok 2018, ss. 429; https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf Białas Andrzej, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT 2007 PN-I-13335:1999, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych

	eResources addresses	Supplementary https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf - J.Wasilewski, Cyberprzestępczość – wybrane aspekty prawnokarne oraz kryminalistyczne, Uniw. w Białymstoku, Białystok 2018 https://wydawnictwo.umk.pl/pl/products/5275/cyberagresja-zjawisko-skutki-zapobieganie - D.Siemieniecka, M.Skibińska, K.Majewska, Cyberagresja – zjawisko, skutki, zapobieganie, UMK 2020 https://www.netcomplex.pl/blog/wp-content/uploads/2016/04/Cyberbezpieczenstwo_Lisiak_Felicka__Szmit.pdf - D.Lisiak-Felicka, M.Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, IASF, Kraków 2016, https://link.springer.com/book/10.1007/978-3-030-78551-2 - K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2022
Example issues/ example questions/ tasks being completed		
Work placement	Not applicable	

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