

**Subject card**

<b>Subject name and code</b>	Cybercrime and cybersecurity - auditorium classes, PG_00132526						
<b>Field of study</b>	Criminology						
<b>Date of commencement of studies</b>	October 2026	<b>Academic year of realisation of subject</b>			2027/2028		
<b>Education level</b>	Master's studies	<b>Subject group</b>			Obligatory subject group in the field of study		
<b>Mode of study</b>	part-time studies	<b>Mode of delivery</b>			at the university		
<b>Year of study</b>	2	<b>Language of instruction</b>			Polish		
<b>Semester of study</b>	3	<b>ECTS credits</b>			1.0		
<b>Learning profile</b>	academic	<b>Assessment form</b>			credit		
<b>Conducting unit</b>	Department of Legal Informatics -> Faculty of Law and Administration -> Rector						
<b>Name and surname of lecturer (lecturers)</b>	<b>Subject supervisor</b>		mgr Patryk Ciurak				
	<b>Teachers</b>						
<b>Lesson types</b>	<b>Lesson type</b>	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	<b>Number of study hours</b>	0.0	10.0	0.0	0.0	0.0	10
	E-learning hours included: 0.0						
<b>Learning activity and number of study hours</b>	<b>Learning activity</b>	Participation in didactic classes included in study plan		Participation in consultation hours		Self-study	SUM
	<b>Number of study hours</b>	10		0.0		15.0	25
<b>Subject objectives</b>	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_UW01] I able to apply theoretical knowledge of criminology and related disciplines to analyse and interpret problems in criminology in a broad sense	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_K05] Is able to independently and critically complement knowledge and skills, extended by the interdisciplinary dimension	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_UW02] Is able to acquire knowledge and develop professional skills independently, using a variety of sources (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
	[KRYMMU2_UW05] Has the ability to independently propose solutions to a specific problem and carry out a procedure to reach a decision on it	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	<p>F.Wołoski, J.Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych, edu-Libri, Warszawa 2012</p> <p>K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2022</p> <p>M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securinum 2023</p> <p>D.Lisiak-Felicka, M.Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, IASF, Kraków 2016, ss. 222; <a href="https://www.netcomplex.pl/blog/wp-content/uploads/2016/04/Cyberbezpieczenstwo_Lisiak_Felicka__Szmit.pdf">https://www.netcomplex.pl/blog/wp-content/uploads/2016/04/Cyberbezpieczenstwo_Lisiak_Felicka__Szmit.pdf</a></p> <p>D.Siemieniecka, M.Skibińska, K.Majewska, Cyberagresja zjawisko, skutki, zapobieganie, UMK 2020, ss. 198; <a href="https://wydawnictwo.umk.pl/pl/products/5275/cyberagresja-zjawisko-skutki-zapobieganie">https://wydawnictwo.umk.pl/pl/products/5275/cyberagresja-zjawisko-skutki-zapobieganie</a></p> <p>M.Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, Wyd. II, PTI, Warszawa 2014; ss. 238; <a href="https://historiainformatyki.pl/historia/dokument.php?nonav=&amp;nrrar=6&amp;nrrresp=6&amp;sygn=V%2F1%2F7&amp;handle=1&amp;folder=1">https://historiainformatyki.pl/historia/dokument.php?nonav=&amp;nrrar=6&amp;nrrresp=6&amp;sygn=V%2F1%2F7&amp;handle=1&amp;folder=1</a></p> <p>J.Wasilewski, Cyberprzestępczość wybrane aspekty prawnokarne oraz kryminalistyczne, Uniw. w Białymstoku, Białystok 2018, ss. 429; <a href="https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf">https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf</a></p> <p>Białas Andrzej, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT 2007</p> <p>PN-I-13335:1999, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych</p>
	eResources addresses	
Example issues/ example questions/ tasks being completed		
Work placement	Not applicable	

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