

Subject card

Subject name and code		Cybercrime and cybersecurity - lecture, PG_00132852						
Field of study		Criminology						
Date of commencement of studies		October 2026	Academic year of realisation of subject			2027/2028		
Education level		Master'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		2	Language of instruction			Polish		
Semester of study		3	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		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_W01] Has an in-depth knowledge of the nature of legal and penal sciences, their place within the system of sciences, their interrelationships, and main development trends.		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_W05] Has an in-depth knowledge of research methods and tools, including techniques of data collection, analysis and interpretation, specific to criminology and forensic science.		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_K05] Is able to independently and critically develop their knowledge and skills, taking into account their interdisciplinary nature.		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		

Subject contents	<p>1. Computer identification on the network: MAC addresses, IP addresses (static, dynamic; private, public), domain whois, network whois, DHCP, NAT, ports, ISP, ICP, IAP, domain (subdomain), hosting, cloud services, role of DNS servers, operator identification.</p> <p>2. Accountability of Internet activities: connection anonymisation, Proxy, VPN, TOR network, Darknet, e-mail anonymisation</p> <p>3. Identification of the elements of computer crime. Examples of cybercrime tools and methods: identity theft, spoofing, passwords and static access data, phishing, man-in-the-middle, spam, whaling (CEO Fraud), misinformation, fake news, SQL/HTML Injection, formjacking, exploit kits, darknet and blockchain</p>		
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	<p>J. Kosiński, Paradygmaty cyberprzestępczości, Difin, Warszawa 2015</p> <p>C.Banasiński, M.Rojszczak, Cyberbezpieczeństwo wyd. 2, WoltersKluwer, Warszawa 2023</p> <p>F.Wołoski, J.Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych, edu-Libri, Warszawa 2012</p>	
	Supplementary literature	<p>K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2021</p> <p>M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securinum 2024</p> <p>M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 2, Securinum 2025</p> <p>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</p> <p>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</p> <p>M.Szmit, Wybrane zagadnienia opiniowania sądowo-informatycznego, Wyd. II, PTI, Warszawa 2014; ss. 238; https://historiainformatyki.pl/historia/dokument.php?nonav=&nrrar=6&nrrzesp=6&sygn=V%2F1%2F7&handle=1&folder=1</p> <p>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</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.