University of Gdańsk

Subject card

Subject name and code	Cybercrime and cybersecurity - lecture, PG_00132527		
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	part-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	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

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_K05] Is able to independently and critically develop their knowledge and skills, taking into account their interdisciplinary nature.	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
[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_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

<table>
<tr><td>Subject contents</td><td>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.

2. Accountability of Internet activities: connection anonymisation, Proxy, VPN, TOR network, Darknet, e-mail anonymisation

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</td></tr>
<tr><td>Prerequisites and co-requisites</td><td></td></tr>
<tr><td>Assessment methods and criteria</td><td><table><tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr><tr><td>test</td><td>51.0%</td><td>100.0%</td></tr></table></td></tr>
<tr><td>Recommended reading</td><td><table><tr><td>Basic literature</td><td>J. Kosiński, Paradygmaty cyberprzestępczości, Difin, Warszawa 2015

C.Banasiński, M.Rojszczak, Cyberbezpieczeństwo wyd. 2, WoltersKluwer, Warszawa 2023

F.Wołowski, J.Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych, edu-Libri, Warszawa 2012</td></tr><tr><td>Supplementary literature</td><td>K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński. Cybersecurity in Poland: legal aspects. Springer 2021

M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 1, Securitum 2024

M. Sajdak (red.), Wprowadzenie do bezpieczeństwa IT. Tom 2, Securitum 2025

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</td></tr><tr><td>eResources addresses</td><td></td></tr></table></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td></td></tr>
<tr><td>Work placement</td><td>Not applicable</td></tr>
</table>

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