Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberprzestępczość i cyberbezpieczeństwo - wykład, PG_00132852		
Kierunek studiów	Kryminologia (O)		
Data rozpoczęcia studiów	październik 2025 r.	Rok akademicki realizacji przedmiotu	2026/2027
Poziom kształcenia	II stopnia	Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	2	Język wykładowy	polski
Semestr studiów	3	Liczba punktów ECTS	2.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
Jednostka prowadząca	Rektor -> Wydział Prawa i Administracji		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	mgr Patryk Ciurak	
	Prowadzący zajęcia z przedmiotu		

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	30.0	0.0	0.0	0.0	0.0	30
W tym liczba godzin zajęć na odległość: 0.0						

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	30	0.0	20.0	50

Cel przedmiotu

Studenci poznają prawne, procesowe i techniczne aspekty przestępstw związanych z technologiami informatycznymi oraz zaznajamiają się z podstawowymi zasadami i mechanizmami bezpieczeństwa systemów informatycznych, jak i z normami prawnymi regulującymi korzystanie z komputerów itp. i sieci teleinformatycznych.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[KRYMMU2_WG05] Ma pogłębioną wiedzę co do sposobów i narzędzi, w tym techniki pozyskiwania danych i informacji, właściwych dla kryminologii i kryminalistyki	Student zna niebezpieczeństwa związane z użytkowaniem komputerów i sieci informatycznych, zasady zarządzania bezpieczeństwem systemów informatycznych, niebezpieczeństwa dotyczące utraty prywatności, zasady ochrony własności intelektualnej oraz podstawy prawa patentowego i autorskiego.	[SW4] test/egzamin - ustny lub pisemny [SW1] wypowiedź ustna/rozmowa/ dyskusja [SW5] realizacja zadania problemowego
[KRYMMU2_WG01] Ma pogłębioną wiedzę o charakterze nauk prawnych oraz związanych z naukami penalnymi, ich miejscu w systemie nauk i wzajemnych relacjach	Student zna niebezpieczeństwa związane z użytkowaniem komputerów i sieci informatycznych, zasady zarządzania bezpieczeństwem systemów informatycznych, niebezpieczeństwa dotyczące utraty prywatności, zasady ochrony własności intelektualnej oraz podstawy prawa patentowego i autorskiego.	[SW4] test/egzamin - ustny lub pisemny [SW1] wypowiedź ustna/rozmowa/ dyskusja [SW5] realizacja zadania problemowego

<table>
<tr><td>Treści przedmiotu</td><td colspan="2">1. Identyfikacja komputera w sieci: adresy MAC, IP (statyczne, dynamiczne; prywatne, publiczne), whois domenowe, sieciowe, DHCP, NAT, porty, ISP, ICP, IAP, domena (subdomena), hosting, usługi chmurowe, rola serwerów DNS, identyfikacja operatora.
2. Rozliczalność działań w sieci Internet: anonimizacja połączeń, Proxy, VPN, sieć TOR, Darknet, anonimizacja poczty elektronicznej
3. Identyfikacja znamion przestępstw komputerowych. Przykłady narzędzi i metod cyberprzestępców: identity theft, spoofing, hasła i statyczne dane dostępowe, phishing, man-in-the-middle, spam, whaling (CEO Fraud), dezinformacja, fake news, SQL/HTML Injection, formjacking, exploit kits, darknet i blockchain</td></tr>
<tr><td>Wymagania wstępne i dodatkowe</td><td colspan="2"></td></tr>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td colspan="2"><table><tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr><tr><td>test</td><td>51.0%</td><td>100.0%</td></tr></table></td></tr>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</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>Uzupełniająca lista lektur</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>Adresy eZasobów</td><td>Adresy na platformie eNauczanie:</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2"></td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="2">Nie dotyczy</td></tr>
</table>

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.