Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Cyberprzestępczość i cyberbezpieczeństwo - wykład, PG_00132527						
Kierunek studiów	Kryminologia (O)						
Data rozpoczęcia studiów	październik 2024 r.		Rok akademicki realizacji przedmiotu	2025/2026			
Poziom kształcenia	II stopnia		Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów			
Forma studiów	niestacjonarne		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 -> Katedra Informatyki Prawniczej						
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	15.0	0.0	0.0	0.0	0.0	15
	W tym liczba godzin zajęć na odległość: 0.0						
	Dodatkowe informacje: Dyskusja Analiza zdarzeń krytycznych (przypadków) Wykład konwersatoryjny Praca w grupach						
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	15	0.0	35.0	50		
Cel przedmiotu	Studenci poznają prawne, procesowe i techniczne aspekty przestępst 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_UW04] Potrafi posługiwać się zasadami i normami prawnymi jak i zawodowymi w podejmowanej działalności kryminologa	Student potrafi znajdować informacje z literatury, Internetu i innych źródeł z dziedziny bezpieczeństwa systemów informatycznych, interpretować w/ w informacje, wyciągać wnioski oraz formułować i uzasadniać opinie, przygotować politykę bezpieczeństwa dla organizacji.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_KR05] Jest gotowy do podejmowania się przygotowania oraz uczestniczenia w przygotowaniu projektów społecznych, uwzględniające aspekty prawne, ekonomiczne i polityczne, w tym przygotowania i realizacji projektów współfinansowanych ze środków Unii Europejskiej	Student nie nadużywa systemów informatycznych naruszając cudzą prywatność, nie dokonuje czynów zabronionych ani nieetycznych związanych z użytkowaniem komputerów i sieci informatycznych, nie używa oprogramowania, do którego nie nabył prawa.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_KR08] Ma świadomość poziomu swojej wiedzy i umiejętności, a także rozumie potrzebę uczenia się przez całe życie	Student nie nadużywa systemów informatycznych naruszając cudzą prywatność, nie dokonuje czynów zabronionych ani nieetycznych związanych z użytkowaniem komputerów i sieci informatycznych, nie używa oprogramowania, do którego nie nabył prawa.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_WG04] Ma rozszerzoną wiedzę o różnych rodzajach przestępczości oraz sposobach ich przeciwdziałania.	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_UW01] Potrafi wykorzystywać wiedzę teoretyczną z zakresu kryminologii oraz powiązanych z nią dyscyplin naukowych w celu analizowania i interpretowania problemów związanych z kryminologią szeroko rozumianą	Student potrafi znajdować informacje z literatury, Internetu i innych źródeł z dziedziny bezpieczeństwa systemów informatycznych, interpretować w/ w informacje, wyciągać wnioski oraz formułować i uzasadniać opinie, przygotować politykę bezpieczeństwa dla organizacji.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_UW05] Potrafi ocenić przydatność typowych procedur i dobrych praktyk do realizacji zadań związanych z różnymi sferami związanymi z kryminologią	Student potrafi znajdować informacje z literatury, Internetu i innych źródeł z dziedziny bezpieczeństwa systemów informatycznych, interpretować w/ w informacje, wyciągać wnioski oraz formułować i uzasadniać opinie, przygotować politykę bezpieczeństwa dla organizacji.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_UW02] Potrafi samodzielnie zdobywać wiedzę i rozwijać swoje profesjonalne umiejętności, korzystając z różnych źródeł (w języku rodzimym i obcym) i nowoczesnych technologi	Student potrafi znajdować informacje z literatury, Internetu i innych źródeł z dziedziny bezpieczeństwa systemów informatycznych, interpretować w/ w informacje, wyciągać wnioski oraz formułować i uzasadniać opinie, przygotować politykę bezpieczeństwa dla organizacji.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU4] test/egzamin - ustny lub pisemny [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[KRYMMU2_KK01] Ma świadomość poziomu swojej wiedzy i umiejętności, a także rozumie potrzebę uczenia się przez całe życie	Student nie nadużywa systemów informatycznych naruszając cudzą prywatność, nie dokonuje czynów zabronionych ani nieetycznych związanych z użytkowaniem komputerów i sieci informatycznych, nie używa oprogramowania, do którego nie nabył prawa.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[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
[KRYMMU2_UK02] Jest przygotowany do aktywnego uczestnictwa w grupach, organizacjach i instytucjach związanych z szeroko pojętą kryminologią, jednocześnie jest zdolny do porozumiewania się z osobami będącymi i nie będącymi specjalistami w kryminologii	Student potrafi znajdować informacje z literatury, Internetu i innych źródeł z dziedziny bezpieczeństwa systemów informatycznych, interpretować w/ w informacje, wyciągać wnioski oraz formułować i uzasadniać opinie, przygotować politykę bezpieczeństwa dla organizacji.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK4] test/egzamin - ustny lub pisemny [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta

Treści przedmiotu

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

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
egzamin	51.0%	100.0%

Zalecana lista lektur

Podstawowa lista lektur	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
Uzupełniająca lista lektur	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
Adresy eZasobów	Uzupełniające Adresy na platformie eNauczanie:

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.