

Karta przedmiotu

Nazwa i kod przedmiotu	Krajowy system cyberbezpieczeństwa (Konwersatorium), PG_00179304						
Kierunek studiów	Bezpieczeństwo narodowe (P)						
Data rozpoczęcia studiów	październik 2024 r.		Rok akademicki realizacji przedmiotu		2024/2025		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć z obszarów nauk humanistycznych lub nauk społecznych		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	1		Język wykładowy		polski		
Semestr studiów	2		Liczba punktów ECTS		2.0		
Profil kształcenia	praktyczny		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Rektor -> Wydział Nauk Społecznych						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr Piotr Robakowski				
	Prowadzący zajęcia z przedmiotu		dr Piotr Robakowski				
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		30.0	60
Cel przedmiotu	Celem przedmiotu Krajowy System Cyberbezpieczeństwa jest dostarczenie studentom wszechstronnej wiedzy na temat struktury, zasad i procedur związanych z zapewnieniem cyberbezpieczeństwa w Polsce, zgodnie z dyrektywą NIS (Network and Information Systems) oraz ustawą o krajowym systemie cyberbezpieczeństwa. Przedmiot obejmuje analizę zagrożeń cybernetycznych, mechanizmy zarządzania ryzykiem, oraz rolę i zadania kluczowych instytucji i podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[BNMU2_U14] Posiada pogłębione umiejętności poszukiwania i dokonywania selekcji źródeł oraz zna w sposób rozszerzony możliwości technologiczne służące do poszukiwania informacji, co wykorzystuje do dalszego własnego rozwoju.	Posiada pogłębione umiejętności poszukiwania i dokonywania selekcji źródeł prawnych z zakresu bezpieczeństwa IT oraz zna w sposób rozszerzony możliwości technologiczne służące do poszukiwania informacji o formach ochrony danych	[SU4] test/egzamin - ustny lub pisemny
	[BNMU2_K01] Jest przygotowany do aktywności na rynku pracy w obszarze bezpieczeństwa, ma świadomość konieczności samodzielnego podnoszenia kwalifikacji, zbierania i analizowania informacji, krytycznie ocenia posiadaną i zdobywaną wiedzę.	Jest przygotowany do aktywności na rynku pracy w obszarze bezpieczeństwa IT, ma świadomość konieczności samodzielnego podnoszenia kwalifikacji, zbierania i analizowania informacji w obszarze oddziaływania cyberprzestrzeni.	[SK1] wypowiedź ustna/rozmowa/dyskusja
	[BNMU2_W11] Ma pogłębioną wiedzę dotyczącą strategii bezpieczeństwa na poziomach wojewódzkim i krajowym.	Ma pogłębioną wiedzę dotyczącą strategii cyberbezpieczeństwa.	[SW4] test/egzamin - ustny lub pisemny
	[BNMU2_W09] Ma pogłębioną i uporządkowaną wiedzę o istocie, dynamice i specyfice zagrożeń bezpieczeństwa w różnych sferach życia społecznego.	Ma pogłębioną i uporządkowaną wiedzę o istocie, dynamice i specyfice zagrożeń cyberbezpieczeństwa w różnych sferach życia społecznego.	[SW4] test/egzamin - ustny lub pisemny
	[BNMU2_U03] W sposób pogłębiony analizuje przyczyny i przebieg procesów oraz ich ewolucji odnoszących się do bezpieczeństwa, prognozuje wyzwania, trendy i zagrożenia dla społecznego, politycznego, prawnego, ekonomicznego i etycznego z wykorzystaniem narzędzi i metod właściwych naukom o bezpieczeństwie	W sposób pogłębiony analizuje przyczyny i przebieg procesów oraz ich ewolucji odnoszących się do cyberbezpieczeństwa, prognozuje wyzwania, trendy i zagrożenia dla społecznego, politycznego, prawnego, ekonomicznego i etycznego aspektu oddziaływania cyberprzestrzeni.	[SU1] wypowiedź ustna/rozmowa/dyskusja

Treści przedmiotu	Wprowadzenie do Cyberbezpieczeństwa		
	- Definicja cyberbezpieczeństwa - Znaczenie cyberbezpieczeństwa w kontekście krajowym i globalnym - Podstawowe pojęcia i terminy związane z cyberbezpieczeństwem		
	2. Ramy Prawne Cyberbezpieczeństwa		
	- Dyrektywa NIS (Network and Information Systems Directive) - Ustawa o krajowym systemie cyberbezpieczeństwa - Inne krajowe i międzynarodowe regulacje prawne dotyczące cyberbezpieczeństwa		
	3. Struktura Krajowego Systemu Cyberbezpieczeństwa		
	- Organizacja i rola kluczowych instytucji (np. CERT Polska, ABW, NASK) - Mechanizmy współpracy międzysektorowej - Rola i obowiązki administracji publicznej, sektora prywatnego i obywateli		
	4. Identyfikacja i Analiza Zagrożeń Cybernetycznych		
	- Typy zagrożeń (np. malware, phishing, ransomware) - Techniki i metody wykorzystywane przez cyberprzestępców - Analiza przypadków ataków cybernetycznych i ich konsekwencje		
	5. Ocena Ryzyka i Zarządzanie Ryzykiem		
	- Metody oceny ryzyka w cyberbezpieczeństwie - Zarządzanie ryzykiem: identyfikacja, analiza, kontrola - Implementacja strategii zarządzania ryzykiem w organizacjach		
Wymagania wstępne i dodatkowe	6. Ochrona Infrastruktury Krytycznej		
	- Definicja i znaczenie infrastruktury krytycznej - Metody ochrony infrastruktury krytycznej przed cyberatakami - Współpraca międzynarodowa w zakresie ochrony infrastruktury krytycznej		
	7. Technologie i Narzędzia Cyberbezpieczeństwa		
	- Przegląd najnowszych technologii i narzędzi do zapewnienia cyberbezpieczeństwa - Systemy detekcji i prewencji ataków (IDS/IPS) - Firewalle, antywirusy, szyfrowanie		
	8. Planowanie i Reagowanie na Incydenty Cybernetyczne		
	- Tworzenie i implementacja planów reagowania na incydenty - Proces zarządzania incydentami: identyfikacja, reakcja, odzyskiwanie - Ćwiczenia i symulacje incydentów cybernetycznych		
	9. Edukacja i Świadomość w Cyberbezpieczeństwie		
	- Programy edukacyjne i szkolenia z zakresu cyberbezpieczeństwa - Podnoszenie świadomości użytkowników i pracowników - Najlepsze praktyki i studia przypadków		
	10. Przyszłość Cyberbezpieczeństwa		
	- Trendy i przyszłe wyzwania w cyberbezpieczeństwie - Rola sztucznej inteligencji i uczenia maszynowego w cyberbezpieczeństwie - Przyszłe zmiany legislacyjne i ich wpływ na cyberbezpieczeństwo		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	case study dyskusja	60.0%	20.0%
	test	60.0%	80.0%

Zalecana lista lektur	Podstawowa lista lektur	• Michael N. Schmitt, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", Cambridge University Press, 2017. • NIS Directive (EU) 2016/1148, "Official Journal of the European Union", 2016. • Ustawa o krajowym systemie cyberbezpieczeństwa, "Dziennik Ustaw Rzeczypospolitej Polskiej", 2018. • Kimberly Kagan, "Cybersecurity in Our Digital Lives", Springer, 2021. • Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
	Uzupełniająca lista lektur	• Andrew Hoffman, "Web Application Security: Exploitation and Countermeasures for Modern Web Applications", O'Reilly Media, 2020. • D. Ben H. Thacker, G. Mark Hardy, "Building a Cyber Resilient Business", Artech House, 2019. • Jason Andress, Steve Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", Syngress, 2020. • Raef Meeuwisse, "Cybersecurity for Beginners", Cyber Simplicity Ltd, 2019.
	Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Ramy Prawne Cyberbezpieczeństwa: - Opisz główne postanowienia Dyrektywy NIS (Network and Information Systems Directive) i ich znaczenie dla krajowego systemu cyberbezpieczeństwa. - Wyjaśnij kluczowe założenia ustawy o krajowym systemie cyberbezpieczeństwa i omów jej wpływ na sektor publiczny i prywatny. Struktura Krajowego Systemu Cyberbezpieczeństwa: - Przedstaw strukturę organizacyjną krajowego systemu cyberbezpieczeństwa, wskazując kluczowe instytucje i ich rolę. - Omów mechanizmy współpracy międzysektorowej w zakresie cyberbezpieczeństwa. Identyfikacja i Analiza Zagrożeń Cybernetycznych: - Scharakteryzuj różne typy zagrożeń cybernetycznych, takie jak malware, phishing, ransomware, i ich potencjalne skutki. - Przeanalizuj przykłady rzeczywistych ataków cybernetycznych i omów ich przebieg oraz konsekwencje. Ocena Ryzyka i Zarządzanie Ryzykiem: - Wyjaśnij metody oceny ryzyka w cyberbezpieczeństwie oraz omów proces zarządzania ryzykiem. - Przedstaw kroki związane z implementacją strategii zarządzania ryzykiem w organizacjach. Ochrona Infrastruktury Krytycznej: - Zdefiniuj pojęcie infrastruktury krytycznej i wyjaśnij jej znaczenie w kontekście cyberbezpieczeństwa. - Omów metody ochrony infrastruktury krytycznej przed cyberatakami i przedstaw przykłady najlepszych praktyk. Technologie i Narzędzia Cyberbezpieczeństwa: - Przedstaw przegląd najnowszych technologii i narzędzi stosowanych w celu zapewnienia cyberbezpieczeństwa, takich jak systemy detekcji i prewencji ataków (IDS/IPS). - Omów rolę firewalli, oprogramowania antywirusowego i szyfrowania w ochronie danych. Planowanie i Reagowanie na Incydenty Cybernetyczne: - Opisz proces tworzenia i implementacji planów reagowania na incydenty cybernetyczne. - Omów etapy zarządzania incydentami, w tym identyfikację, reakcję i odzyskiwanie danych po incydencie. Edukacja i Świadomość w Cyberbezpieczeństwie: - Przedstaw znaczenie edukacji i szkoleń z zakresu cyberbezpieczeństwa dla pracowników i użytkowników. - Omów najlepsze praktyki w zakresie podnoszenia świadomości na temat zagrożeń cybernetycznych. Międzynarodowe Aspekty Cyberbezpieczeństwa: - Wyjaśnij zasady transferu danych osobowych do krajów trzecich zgodnie z RODO i Dyrektywą NIS. - Omów rolę międzynarodowej współpracy w zakresie ochrony cyberprzestrzeni. Przyszłość Cyberbezpieczeństwa: - Przeanalizuj przyszłe trendy i wyzwania w cyberbezpieczeństwie, w tym rolę sztucznej inteligencji i uczenia maszynowego. - Przedstaw przewidywane zmiany legislacyjne i ich potencjalny wpływ na cyberbezpieczeństwo.
Praktyki zawodowe w ramach przedmiotu	Realizowane w trakcie praktyk studenckich w instytucjach administracji publicznej.

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.