Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo informacyjne (Wykład), PG_00205429						
Kierunek studiów	Bezpieczeństwo narodowe (P)						
Data rozpoczęcia studiów	październik 2027 r.		Rok akademicki realizacji przedmiotu	2027/2028			
Poziom kształcenia	I stopnia - licencjackie		Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z praktycznym przygotowaniem zawodowym - profil praktyczny			
Forma studiów	stacjonarne		Sposób realizacji	na uczelni			
Rok studiów	1		Język wykładowy	polski			
Semestr studiów	2		Liczba punktów ECTS	1.0			
Profil kształcenia	praktyczny		Forma zaliczenia	zaliczenie			
Jednostka prowadząca	Rada Uczelni						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr Konrad Ćwikliński				
	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						
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	10.0		25

Cel przedmiotu	Celem przedmiotu Bezpieczeństwo informacyjne w formie ćwiczeń audytoryjnych jest przygotowanie studentów do rozumienia, analizowania i praktycznego rozwiązywania problemów związanych z bezpieczeństwem informacji w kontekście funkcjonowania państwa, instytucji publicznych oraz podmiotów prywatnych. Przedmiot ma na celu wykształcenie umiejętności identyfikacji zagrożeń informacyjnych, oceny ryzyka oraz stosowania środków zaradczych, w tym organizacyjnych, technicznych i prawnych. Szczególny nacisk położony zostanie na rozwijanie kompetencji w zakresie ochrony danych, cyberbezpieczeństwa, zarządzania incydentami bezpieczeństwa oraz analizowania współczesnych zagrożeń hybrydowych i dezinformacyjnych. W ramach ćwiczeń studenci zapoznają się z praktycznymi aspektami bezpieczeństwa informacyjnego od podstaw analizy informacji i oceny wiarygodności źródeł, przez modelowanie zagrożeń, po opracowanie procedur reagowania i zabezpieczania systemów informacyjnych. Ćwiczenia obejmują analizę rzeczywistych przypadków naruszeń bezpieczeństwa, tworzenie planów bezpieczeństwa informacyjnego, a także rozwiązywanie zadań symulacyjnych i problemowych.

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[BNL3_U06] Potrafi analizować przyczyny i skutki zagrożeń bezpieczeństwa oraz wskazuje środki zaradcze. Planuje pracę własną oraz zespołu w zakresie analizy zagrożeń i szacowania ryzyka.	Potrafi analizować przyczyny i skutki zagrożeń bezpieczeństwa oraz wskazuje środki zaradcze. Planuje pracę własną oraz zespołu w zakresie analizy zagrożeń i szacowania ryzyka.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[BNL3_W08] W zaawansowanym stopniu wie jakie są mechanizmy w zarządzaniu ryzykiem i podejmowaniu decyzji w instytucjach bezpieczeństwa narodowego.	W zaawansowanym stopniu wie, jakie są mechanizmy i identyfikuje je w zarządzaniu ryzykiem i podejmowaniu decyzji w instytucjach bezpieczeństwa narodowego.	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport [SW5] realizacja zadania problemowego
	[BNL3_W11] Ma zaawansowaną wiedzę dotyczącą strategii bezpieczeństwa na poziomie wojewódzkim i krajowym.	Ma zaawansowaną wiedzę dotyczącą strategii bezpieczeństwa na poziomie wojewódzkim i krajowym.	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport [SW5] realizacja zadania problemowego
	[BNL3_W13] Posiada wiedzę z zakresu prawa własności intelektualnej, obejmującą ochronę praw autorskich oraz własności przemysłowej.	Zna i rozumie zasady prawa własności intelektualnej. Posiada wiedzę z zakresu ochrony praw autorskich i ochrony własności przemysłowej.	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport [SW5] realizacja zadania problemowego
	[BNL3_K04] Jest przygotowana do aktywności na rynku pracy, ma świadomość konieczności podnoszenia kwalifikacji odpowiedzialnego pełnienia ról zawodowych.	Jest przygotowany do aktywności na rynku pracy, ma świadomość konieczności podnoszenia kwalifikacji i odpowiedzialnego pełnienia ról zawodowych.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta
	[BNL3_U05] Wskazuje i wyjaśnia rolę państwa demokratycznego, a także społeczeństwa obywatelskiego w obszarze bezpieczeństwa.	Wskazuje i wyjaśnia rolę państwa demokratycznego, a także społeczeństwa obywatelskiego w obszarze bezpieczeństwa.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[BNL3_U07] Aktywnie uczestniczy w życiu społeczno-politycznym oraz podejmuje próby uczestnictwa w dyskursie publicznym. Kieruje procesem samokształcenia rozwija swój warsztat pracy oraz nowe umiejętności poznawcze. Planuje i organizuje pracę swoją i zespołu, przygotowując projekty społeczne, polityczne, ekonomiczne, obywatelskie (także te, które polegają na współdziałaniu z innymi osobami), korzystając z różnych źródeł i możliwości technologicznych.	Aktywnie uczestniczy w życiu społeczno-politycznym oraz podejmuje próby uczestnictwa w dyskursie publicznym. Planuje i organizuje pracę swoją i zespołu, przygotowując projekty społeczne, polityczne, ekonomiczne i obywatelskie, korzystając z różnych źródeł i technologii.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU5] realizacja zadania problemowego [SU8] obserwacja samodzielnej lub zespołowej pracy studenta

Treści przedmiotu	Ramowy program przedmiotu: Bezpieczeństwo informacyjne (forma: wykład) 1. Wprowadzenie do problematyki bezpieczeństwa informacyjnego • Definicje podstawowe: informacja, bezpieczeństwo, dane, wiedza • Różnica między bezpieczeństwem informacyjnym a cyberbezpieczeństwem • Miejsce bezpieczeństwa informacyjnego w systemie bezpieczeństwa narodowego i międzynarodowego 2. 3. Informacja jako zasób strategiczny • Znaczenie informacji w społeczeństwie sieciowym i informacyjnym • Informacja jako narzędzie władzy, wpływu i kontroli • Zarządzanie informacją modele i strategie 4. 5. Podstawy prawne bezpieczeństwa informacyjnego • Ustawy i regulacje krajowe (RODO, ustawa o ochronie informacji niejawnych) • Normy międzynarodowe i unijne (np. GDPR, NIS2) • Odpowiedzialność instytucjonalna i indywidualna 6. 7. Zagrożenia informacyjne typologie i klasyfikacje • Dezinformacja, propaganda, fake news, manipulacja medialna • Cyberataki, wycieki danych, szpiegostwo cyfrowe • Psychologiczne i socjologiczne aspekty zagrożeń informacyjnych 8. 9. Infrastruktura krytyczna a bezpieczeństwo informacyjne • Czym jest infrastruktura krytyczna informacyjna • Wpływ awarii systemów informacyjnych na funkcjonowanie państwa i społeczeństwa • Modele zabezpieczeń infrastruktury informacyjnej 10. 11. Instytucje odpowiedzialne za bezpieczeństwo informacyjne • Rola państwa, służb specjalnych, wojska, administracji publicznej • CERT, CSIRT, ABW, NASK struktury i kompetencje • Współpraca międzynarodowa i międzyinstytucjonalna 12. Ochrona danych osobowych i prywatności • Pojęcie prywatności i dane osobowe w dobie cyfrowej • Podstawowe zasady ochrony danych (RODO) • Praktyki bezpiecznego przetwarzania i przechowywania danych 13. Cyberbezpieczeństwo jako komponent bezpieczeństwa informacyjnego • Cyberprzestrzeń i cyberzagrożenia • Ataki DDoS, phishing, ransomware przykłady i mechanizmy • Polityki cyberbezpieczeństwa 14. Wojna informacyjna i operacje wpływu • Pojęcie wojny informacyjnej aspekty historyczne i współczesne • Operacje psychologiczne (PSYOPS), narracje i memetyka • Przykłady z Rosji, Chin, Bliskiego Wschodu, NATO 15. Media, dziennikarstwo i bezpieczeństwo informacyjne • Etyka mediów i odpowiedzialność dziennikarska • Manipulacja informacjami w mediach tradycyjnych i społecznościowych • Algorytmy, bańki informacyjne i radykalizacja 16. Sztuczna inteligencja a informacja • Rola sztucznej inteligencji w zarządzaniu i analizie informacji • Deepfakes, generatywna AI, boty i ich wpływ na dezinformację • Etyczne wyzwania technologiczne 17. Polityka informacyjna państwa • Przykłady polityk informacyjnych w wybranych krajach • Strategiczne zarządzanie informacją w kryzysach i konfliktach • Rola rzecznika prasowego, kanałów oficjalnych i komunikacji kryzysowej 18. Edukacja i świadomość informacyjna społeczeństwa • Media literacy, cyfrowa higiena, kultura informacyjna • Programy edukacyjne w szkołach i uczelniach • Społeczna odporność na manipulację 19. Analiza przypadków (case studies) • Studium przypadków: ataki informacyjne, wycieki danych, operacje wpływu • Dyskusja i analiza błędów, strategii i skutków • Wnioski i dobre praktyki

	20. Podsumowanie i przygotowanie do zaliczenia • Powtórzenie głównych pojęć i tematów • Sesja pytań i odpowiedzi • Konsultacje dotyczące zaliczenia przedmiotu
Wymagania wstępne i dodatkowe	Wymagania wstępne: zakres wiadomości, umiejętności i kompetencji 1. Wymagana wiedza i umiejętności przed rozpoczęciem zajęć: Przed przystąpieniem do wykładu z przedmiotu Bezpieczeństwo informacyjne, student powinien posiadać: • Podstawową wiedzę z zakresu nauk społecznych i politycznych, w szczególności dotyczącą funkcjonowania państwa, instytucji publicznych, zasad demokracji i rządzenia. • Ogólną orientację w zagadnieniach bezpieczeństwa narodowego i międzynarodowego, w tym znajomość podstawowych pojęć jak: bezpieczeństwo wewnętrzne, zagrożenia asymetryczne, cyberbezpieczeństwo. • Umiejętność krytycznego myślenia i analizy tekstów naukowych, interpretowania danych i informacji pochodzących z różnych źródeł. • Kompetencje cyfrowe na poziomie średniozaawansowanym, pozwalające na swobodne korzystanie z Internetu, podstawowych narzędzi informatycznych i środowisk edukacyjnych online (np. Moodle, Teams, eUczelnia). • Podstawy prawa, zwłaszcza prawa konstytucyjnego oraz elementy prawa ochrony danych osobowych i dostępu do informacji publicznej. 2. Wymagane zaliczenie innych przedmiotów (jeśli dotyczy): Wskazane jest wcześniejsze zaliczenie przynajmniej jednego z poniższych przedmiotów (lub ich odpowiedników programowych): • Wprowadzenie do bezpieczeństwa narodowego lub wewnętrznego, • Wiedza o państwie i prawie, • Podstawy politologii, • Podstawy systemów informacyjnych w administracji/publicznych instytucjach, • Cyberbezpieczeństwo podstawy (jeśli oferowane wcześniej w programie).
Sposoby i kryteria oceniania osiąganych efektów uczenia się	

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Uczestnictwo w wykładach i samodzielna praca studenta (np. analiza przypadków, dyskusje w trakcie zajęć)	50.0%	50.0%
Aktywność na wykładach i praca własna (np. analiza przypadków, dyskusje):	50.0%	50.0%

Zalecana lista lektur	Podstawowa lista lektur	Literatura podstawowa (publikacje polskojęzyczne) 1. Olejnik, S., Bezpieczeństwo informacyjne państwa, Wydawnictwo Naukowe PWN, Warszawa, 2022. 2. Wojciechowski, S., Bezpieczeństwo informacyjne w stosunkach międzynarodowych, Difin, Warszawa, 2020. 3. Kulesza, J., Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer, Warszawa, 2021. 4. Cieślak, M., Dezinformacja jako zagrożenie dla bezpieczeństwa państwa, Wydawnictwo Naukowe Uniwersytetu Wrocławskiego, Wrocław, 2021. 5. Piechowiak-Lamparska, J., Wojna informacyjna: teoria i praktyka, Uniwersytet Mikołaja Kopernika, Toruń, 2020. 6. Banasik, M., Wojna informacyjna i wojna poznawcza, Wydawnictwo Difin, Warszawa, 2023. Literatura podstawowa (publikacje anglojęzyczne) 1. Castells, M., The Rise of the Network Society (The Information Age: Economy, Society and Culture, Vol. 1), Wiley-Blackwell, Oxford, 2010. 2. Rid, T., Active Measures: The Secret History of Disinformation and Political Warfare, Farrar, Straus and Giroux, New York, 2020. 3. Singer, P.W., Brooking, E.T., LikeWar: The Weaponization of Social Media, Houghton Mifflin Harcourt, Boston, 2018. 4. Kello, L., The Virtual Weapon and International Order, Yale University Press, New Haven, 2017. 5. Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, New York, 2019. 6. Nye, J.S., Soft Power: The Means to Success in World Politics, PublicAffairs, New York, 2004. 7. Geers, K. (ed.), Strategic Cyber Security, NATO CCD COE Publications, Tallinn, 2011.

	Uzupełniająca lista lektur	Literatura uzupełniająca (polskojęzyczna) 1. Marciniak, T., Cyberterroryzm i cyberwojna we współczesnym świecie, Difin, Warszawa, 2020. 2. Kozłowski, A., Bezpieczeństwo cyfrowe państwa, Wydawnictwo Naukowe UAM, Poznań, 2019. 3. Piech, K., Zarządzanie informacją w administracji publicznej, CeDeWu, Warszawa, 2018. 4. Świderska, M., Dezinformacja jako narzędzie walki politycznej, ASPRA-JR, Warszawa, 2016. 5. Szubrycht, T. (red.), Bezpieczeństwo informacyjne. Konteksty teorii i praktyki, Wydawnictwo WAT, Warszawa, 2021. Literatura uzupełniająca (anglojęzyczna) 1. Newman, N., Fletcher, R., Kalogeropoulos, A., Reuters Institute Digital News Report 2024, Reuters Institute, Oxford, 2024. 2. Lin, H., Cybersecurity Ethics, Oxford University Press, Oxford, 2021. 3. Moore, M., Tambini, D. (eds.), Digital Dominance: The Power of Google, Amazon, Facebook, and Apple, Oxford University Press, Oxford, 2018. 4. Paul, C., Information Operations Doctrine and Practice: A Reference Handbook, Praeger, Santa Barbara, 2008. 5. West, D.M., The Future of Work: Robots, AI, and Automation, Brookings Institution Press, Washington D.C., 2018.
	Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Przykładowe zagadnienia do dyskusji lub egzaminu: 1. Różnice między bezpieczeństwem informacyjnym a cyberbezpieczeństwem. 2. Informacja jako narzędzie władzy i kontroli analiza współczesnych przykładów. 3. Dezinformacja i fake news jako zagrożenie dla bezpieczeństwa państwa. 4. Struktura i kompetencje instytucji odpowiedzialnych za bezpieczeństwo informacyjne w Polsce. 5. Wpływ sztucznej inteligencji i deepfakeów na manipulację informacyjną. 6. Rola społeczeństwa informacyjnego w zwiększaniu odporności na zagrożenia informacyjne. 7. Podstawy prawne ochrony danych osobowych porównanie RODO i GDPR. 8. Strategie wojny informacyjnej stosowane przez Rosję i Chiny. 9. Etyczne wyzwania związane z wykorzystaniem danych w polityce i marketingu. 10. Polityka informacyjna państwa w sytuacjach kryzysowych i konfliktowych Przykładowe pytania testowe lub egzaminacyjne 1. Wyjaśnij pojęcie informacja strategiczna i podaj przykład jej zastosowania. 2. Wymień i opisz trzy główne typy zagrożeń informacyjnych. 3. Jakie są kluczowe zasady przetwarzania danych osobowych zgodnie z RODO? 4. Jak działa operacja wpływu w kontekście mediów społecznościowych? 5. Scharakteryzuj rolę instytucji CERT i CSIRT w systemie bezpieczeństwa informacyjnego. 6. W jaki sposób media społecznościowe wpływają na polaryzację społeczną i bezpieczeństwo informacyjne? 7. Jakie środki ochrony informacji stosuje administracja publiczna? 8. Na czym polega zjawisko infodemia i jakie są jego konsekwencje? Przykładowe zadania praktyczne (dla chętnych lub rozszerzonych grup): 1. Analiza studium przypadku Przeanalizuj przykład wycieku danych z instytucji publicznej i wskaż błędy w zarządzaniu bezpieczeństwem informacji. 2. Krytyczna analiza treści medialnej Wskaż elementy manipulacji i dezinformacji w artykule lub poście w mediach społecznościowych. 3. Mapowanie zagrożeń informacyjnych Przygotuj mapę najczęstszych zagrożeń informacyjnych dla administracji publicznej lub sektora zdrowia. 4. Debata akademicka Czy sztuczna inteligencja zagraża wolności informacyjnej jednostki? Przygotuj argumenty za i przeciw. 5. Symulacja komunikacji kryzysowej Przygotuj i zaprezentuj komunikat prasowy instytucji państwowej po cyberataku.
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.