

KARTA PRZEDMIOTU (SYLABUS)

Opis przedmiotu

Kod przedmiotu		Nazwa przedmiotu	Cyberbezpieczeństwo systemów	
AIwB/O/I/NST/B1-37a			Cybersecurity of systems	
Język wykładowy		Polski		
Rok akademicki		2026/2027		
Kierunek		Sztuczna Inteligencja w Biznesie		
w zakresie		-		
Poziom studiów		studia pierwszego stopnia		
Profil studiów		ogólnoakademicki		
Forma studiów		studia niestacjonarne		
Semestr / semestry		semestr czwarty		
Przynależność do grupy zajęć		B. Grupa zajęć kierunkowych B1. Grupa zajęć kierunkowych wybieralnych		
Status przedmiotu		Wybieralny		
Formy realizacji zajęć dydaktycznych, wymiar, punkty ECTS		Forma zajęć	Liczba godzin zajęć dydaktycznych	Liczba punktów ECTS
		Wykład	10 [h]	3,5 ECTS
		Ćwiczenia	[h]	
		Laboratorium	15 [h]	
Powiązanie przedmiotu	z profilem studiów	Związany z prowadzoną działalnością naukową w dyscyplinie informatyka techniczna i telekomunikacja		3 ECTS
	z uprawnieniami			ECTS
	z dyscypliną	Informatyka techniczna i telekomunikacja		3,5 ECTS
Forma nauczania		Tradycyjna - zajęcia zorganizowane w Uczelni/ zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość		
Wymagania wstępne		Wymagana znajomość z przedmiotu analiza matematyka, bardzo dobra znajomość podstawy programowania.		
Jednostka prowadząca		Katedra Biznesu i Finansów Międzynarodowych		
Koordynator		Dr inż. Jacek Wołoszyn		
Adres strony internetowej pjo		http://weif.uniwersytetradom.pl		
Adres e-mail, telefon koordynatora		Jacek.woloszyn@urad.edu.pl (48) 361-7410		

**EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE, REALIZACJA ZAJĘĆ DYDAKTYCZNYCH,
WERYFIKACJA EFEKTÓW UCZENIA SIĘ**

Cel kształcenia:	Celem kształcenia jest zapoznanie studentów z podstawowymi zagadnieniami cyberbezpieczeństwa systemów informatycznych, w tym z metodami identyfikacji zagrożeń, technikami ochrony danych oraz mechanizmami zabezpieczania systemów i sieci komputerowych przed nieautoryzowanym dostępem, atakami oraz utratą integralności informacji.
Treści programowe:	<p>Treści zajęć są powiązane z prowadzonymi badaniami naukowymi.</p> <p>Treści wykładów:</p> <p>Podstawowe pojęcia i znaczenie cyberbezpieczeństwa w systemach informatycznych. Rodzaje zagrożeń i ataków na systemy komputerowe (np. malware, phishing, ataki sieciowe, ataki na aplikacje webowe). Podstawowe mechanizmy ochrony systemów i danych: uwierzytelnianie, autoryzacja, szyfrowanie oraz kontrola dostępu. Bezpieczeństwo sieci komputerowych i komunikacji w Internecie. Zarządzanie bezpieczeństwem informacji oraz polityki bezpieczeństwa w organizacjach. Bezpieczeństwo systemów operacyjnych oraz aplikacji. Podstawy kryptografii i jej zastosowania w ochronie danych. Ochrona danych osobowych oraz aspekty prawne cyberbezpieczeństwa (np. RODO). Przegląd narzędzi i technologii stosowanych w ochronie systemów informatycznych. Suma: 10 [h]</p> <p>Treść laboratoriów:</p> <p>Konfiguracja podstawowych mechanizmów bezpieczeństwa w systemach informatycznych. Analiza podatności systemów i identyfikacja zagrożeń. Wykorzystanie narzędzi do monitorowania bezpieczeństwa oraz analizy ruchu sieciowego. Podstawy kryptografii w praktyce – szyfrowanie i deszyfrowanie danych. Konfiguracja mechanizmów uwierzytelniania i kontroli dostępu. Analiza przykładowych scenariuszy ataków oraz sposoby ich wykrywania i zapobiegania. Podstawy testów bezpieczeństwa systemów informatycznych. Przygotowanie prostych procedur zwiększających poziom bezpieczeństwa systemów i aplikacji. Suma: 15 [h]</p>
Metody dydaktyczne (kształcenia):	<ul style="list-style-type: none"> - metody podające (wykład informacyjny), - metody programowane (z wykorzystaniem komputera), - Obserwacja <p>Zajęcia prowadzone w programie Python3. a także wykorzystanie Biblioteki Numpy, Pandas, Matplotlib, Scikit-learn Tensorflow, Pytorch,</p>
	<p>Warunkiem zaliczenia przedmiotu jest osiągnięcie wszystkich wymaganych efektów uczenia się określonych dla danego przedmiotu. Uzyskanie pozytywnych ocen ze wszystkich form zajęć wchodzących w skład danego przedmiotu jest równoznaczne z jego zaliczeniem i zdobyciem przez studenta liczby punktów ECTS przyporządkowanej temu przedmiotowi.</p> <p>Sposób obliczenia oceny końcowej z przedmiotu określa regulamin studiów.</p> <p>Sposób obliczania oceny z poszczególnych form zajęć przedstawia się następująco:</p> <p>Na ocenę z laboratorium składa się: punktowa ocena wykonanego projektu</p> <p>Na ocenę z wykładu składa się wynik otwartego testu pisemnego.</p> <p>Ocena z egzaminu – wynik otwartego testu pisemnego.</p> <p>Zdobyte w poszczególnych formach zajęć punkty przeliczane zostają na ocenę wg skali:</p> <p>Ocena 2 poniżej 51%</p> <p>Ocena 3 od 51%</p>

	Ocena 3,5 od 61% Ocena 4 od 71% Ocena 4,5 od 81% Ocena 5 od 91%
--	--

Efekty uczenia się dla przedmiotu w odniesieniu do efektów kierunkowych i formy zajęć				Metody weryfikacji efektów uczenia się	
Numer efektu uczenia się	Opis efektów uczenia się dla przedmiotu (PEU) Student, który zaliczył przedmiot (W) zna i rozumie/ (U) potrafi / (K) jest gotów do:	Kierunkowy efekt uczenia się (KEU)	Forma zajęć	Forma weryfikacji (zaliczeń)	Metody sprawdzania i oceny
W1	zna i rozumie podstawowe zagrożenia bezpieczeństwa systemów informatycznych oraz metody ich wykrywania i zapobiegania.	K_W03 K_W05 K_W09	wykład	Zaliczenie na ocenę	pisemny test otwarty
W2	zna i rozumie mechanizmy ochrony danych i systemów, w tym podstawowe metody kryptografii, uwierzytelniania oraz kontroli dostępu.	K_W03 K_W05 K_W09	wykład	Zaliczenie na ocenę	pisemny test otwarty
U1	potrafi identyfikować podstawowe podatności systemów informatycznych oraz analizować potencjalne zagrożenia bezpieczeństwa.	K_U05 K_U09	laboratorium	Zaliczenie na ocenę	ocena zadań laboratoryjnych
U2	potrafi stosować wybrane narzędzia i techniki zwiększające bezpieczeństwo systemów, sieci oraz danych	K_U05 K_U09	laboratorium	Zaliczenie na ocenę	ocena zadań laboratoryjnych
K1	jest gotów do przestrzegania zasad bezpieczeństwa informacji oraz odpowiedzialnego korzystania z systemów informatycznych.	K_K02 K_K05	Wykład/ laboratorium	Zaliczenie na ocenę	Obserwacja, aktywność na zajęciach obserwacja
K2	jest gotów do ciągłego aktualizowania wiedzy w zakresie zagrożeń cyberbezpieczeństwa oraz metod ochrony systemów informatycznych.	K_K02 K_K05	Wykład/ laboratorium	Zaliczenie na ocenę	Obserwacja, aktywność na zajęciach obserwacja

Literatura i pomoce naukowe
<p>Literatura podstawowa:</p> <ol style="list-style-type: none"> 1. Stallings W., <i>Effective Cybersecurity: A Guide to Using Best Practices and Standards</i>, Addison-Wesley, 2018. 2. Anderson R., <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i>, 3rd Edition, Wiley, 2020. 3. Bishop M., <i>Computer Security: Art and Science</i>, 2nd Edition, Addison-Wesley, 2018. 4. Whitman M. E., Mattord H. J., <i>Principles of Information Security</i>, 7th Edition, Cengage Learning, 2021. 5. Kurose J. F., Ross K. W., <i>Computer Networking: A Top-Down Approach</i>, 8th Edition, Pearson, 2021. 6. Schneier B., <i>Secrets and Lies: Digital Security in a Networked World</i>, Wiley, 2015. <p>Literatura uzupełniająca:</p> <ol style="list-style-type: none"> 1. Goodrich M. T., Tamassia R., <i>Introduction to Computer Security</i>, 2nd Edition, Pearson, 2019. 2. Easttom C., <i>Network Defense and Countermeasures</i>, 2nd Edition, Pearson, 2018. 3. Kim D., Solomon M., <i>Fundamentals of Information Systems Security</i>, 3rd Edition, Jones & Bartlett Learning, 2021. 4. Vacca J. R., <i>Computer and Information Security Handbook</i>, 3rd Edition, Elsevier, 2017. 5. Gruszczyk A., <i>Cyberbezpieczeństwo w teorii i praktyce</i>, Difin, Warszawa, 2020. 6. Clarke R., Knake R., <i>Cyber War: The Next Threat to National Security and What to Do About It</i>, HarperCollins, 2019. 7. 21st Century Computer Science - Challenges and Dilemmas : Artificial Intelligence - The Future of IT. (2025). W J. W. Wołoszyn & A. M. Molga (Redaktorzy), Monografie - Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego (No. 345; s. 155). Uniwersytet Radomski im. Kazimierza Pułaskiego. https://katalog.uniwersytetradom.pl/1783601768532/ksiazka/21st-century-computer-science-challenges-and-dilemmas?bibFilter=178

8. Molga, A. M., & Wołoszyn, J. W. (2025). AI and Cybersecurity-Will AI Become the Shield of the Network? *Dydaktyka Informatyki*, Article 20. <https://doi.org/10.15584/di.2025.20.5>
Szczegółowy wykaz dodatkowych źródeł i pomocy naukowych na pierwszych zajęciach podaje prowadzący.

Nakład pracy studenta potrzebny do osiągnięcia zakładanych efektów uczenia się – bilans punktów ECTS		
Udział w zajęciach, aktywność	Obciążenie studenta [h]	
	Praca własna studenta - zajęcia bez nauczyciela (ZBN)	Zajęcia dydaktyczne
Udział w wykładach i laboratoriach	X	25 [h]
Przygotowanie do <i>zajęć</i> , Przygotowanie do <i>zaliczenia</i>	63 [h]	X
Sumaryczne obciążenie pracą studenta	63[h]/ 2,5 ECTS	25 [h]/ 1 E CTS
Punkty ECTS za przedmiot	3,5 ECTS	

Informacje dodatkowe, uwagi
<p>W przypadku studentów ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekle chorych, określone powyżej (w karcie) metody i formy weryfikacji efektów uczenia się dostosowuje się odpowiednio do indywidualnych potrzeb tych studentów.</p> <p>Szczegółowe zasady i formy wsparcia studentów ze szczególnymi potrzebami: w tym z niepełnosprawnością, przewlekle chorych podczas zajęć, zaliczeń i egzaminów określono w: Regulaminie Studiów, Zasadach Studiowania, Procedurze dotyczącej zapewnienia dostępności procesu kształcenia studentom ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekle chorych.</p>