

# KARTA PRZEDMIOTU (SYLABUS)

## Opis przedmiotu

Kod przedmiotu		Nazwa przedmiotu	Elementy bezpieczeństwa sieci	
AIWB/O/II/ST/B1-17			Network security elements	
Język wykładowy		Polski		
Rok akademicki		2026/2027		
Kierunek		Sztuczna Inteligencja w Biznesie		
w zakresie		-		
Poziom studiów		studia drugiego stopnia		
Profil studiów		ogólnoakademicki		
Forma studiów		studia stacjonarne		
Semestr / semestry		semestr drugi		
Przynależność do grupy zajęć		B. Grupa zajęć kierunkowych B1. Grupa zajęć kierunkowych obowiązkowych		
Status przedmiotu		Obowiązkowy		
Formy realizacji zajęć dydaktycznych, wymiar, punkty ECTS		Forma zajęć	Liczba godzin zajęć dydaktycznych	Liczba punktów ECTS
		Wykład	30 [h]	4 ECTS
		Ćwiczenia	[h]	
		Konwersatorium	[h]	
		Laboratorium	30 [h]	
Powiązanie przedmiotu	z profilem studiów	Związany z prowadzoną działalnością naukową w dyscyplinie Informatyka techniczna i telekomunikacja		2 ECTS
	z uprawnieniami			ECTS
	z dyscypliną	Informatyka techniczna i telekomunikacja		4 ECTS
Forma nauczania		tradycyjna- zajęcia zorganizowane w Uczelni / zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość		
Wymagania wstępne		Znajomość podstawowej obsługi komputera niezbędna dla wykonania ćwiczeń laboratoryjnych.		
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 przedmiotu jest zapoznanie studentów z podstawowymi zagadnieniami bezpieczeństwa sieci komputerowych oraz rozwinięcie umiejętności identyfikowania zagrożeń, stosowania mechanizmów ochrony i konfigurowania podstawowych zabezpieczeń w infrastrukturze sieciowej.
Treści programowe:	<p>Treści zajęć są powiązane z prowadzonymi badaniami naukowymi.</p> <p><b>Treści wykładów:</b></p> <ol style="list-style-type: none"> <li>1. Wprowadzenie do bezpieczeństwa sieci komputerowych – podstawowe pojęcia i modele bezpieczeństwa.</li> <li>2. Rodzaje zagrożeń w sieciach komputerowych – ataki sieciowe, malware, socjotechnika.</li> <li>3. Mechanizmy uwierzytelniania i autoryzacji w sieciach komputerowych.</li> <li>4. Podstawy kryptografii w bezpieczeństwie sieci – szyfrowanie symetryczne i asymetryczne, funkcje skrótu.</li> <li>5. Protokoły bezpieczeństwa w sieciach komputerowych (np. SSL/TLS, IPsec, VPN).</li> <li>6. Zapory sieciowe (firewall) i systemy wykrywania włamań (IDS/IPS).</li> <li>7. Bezpieczeństwo sieci bezprzewodowych.</li> <li>8. Zarządzanie bezpieczeństwem i polityki bezpieczeństwa w organizacji.</li> <li>9. Monitorowanie i analiza ruchu sieciowego pod kątem zagrożeń.</li> <li>10. Aktualne zagrożenia i trendy w bezpieczeństwie sieci.</li> </ol> <p>Suma: 8 [h]</p> <p><b>Treść laboratoriów:</b></p> <ol style="list-style-type: none"> <li>1. Konfiguracja podstawowych mechanizmów bezpieczeństwa w systemach i sieciach komputerowych.</li> <li>2. Analiza ruchu sieciowego z wykorzystaniem narzędzi do monitorowania sieci.</li> <li>3. Konfiguracja zapory sieciowej i podstawowych reguł bezpieczeństwa.</li> <li>4. Implementacja bezpiecznych połączeń z wykorzystaniem protokołów szyfrowania.</li> <li>5. Konfiguracja i testowanie sieci VPN.</li> <li>6. Analiza przykładowych ataków sieciowych i sposobów ich wykrywania.</li> <li>7. Zabezpieczanie sieci bezprzewodowej.</li> <li>8. Wykorzystanie narzędzi do skanowania podatności i testowania bezpieczeństwa.</li> <li>9. Konfiguracja i analiza działania systemów IDS/IPS.</li> <li>10. Projekt laboratoryjny – analiza i poprawa bezpieczeństwa przykładowej infrastruktury sieciowej.</li> </ol> <p>Suma: 15 [h]</p>
Metody dydaktyczne (kształcenia):	<ul style="list-style-type: none"> <li>- metody podające (wykład informacyjny),</li> <li>- metody programowane (z wykorzystaniem komputera),</li> <li>- Obserwacja</li> </ul>
	Warunkiem zaliczenia przedmiotu jest osiągnięcie wszystkich wymaganych efektów uczenia się określonych dla 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. Sposób obliczenia oceny końcowej z przedmiotu określony został zarządzeniem Rektora URad.

	<p>Sposób obliczania oceny z poszczególnych form zajęć przedstawia się następująco:</p> <p>Ocena z laboratorium: test lub projekt</p> <p>Na ocenę z wykładu składa się wynik otwartego testu pisemnego.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 występujące w sieciach komputerowych oraz mechanizmy ich wykrywania i ograniczania.	K_W09 K_W10	wykład	Zaliczenie na ocenę	pisemny test otwarty
W2	zna i rozumie zasady działania wybranych metod i narzędzi służących do zabezpieczania sieci komputerowych, w tym mechanizmów kryptograficznych i protokołów bezpieczeństwa.	K_W09 K_W10	wykład	Zaliczenie na ocenę	pisemny test otwarty
U1	potrafi identyfikować podstawowe zagrożenia bezpieczeństwa w sieci komputerowej oraz analizować ruch sieciowy pod kątem potencjalnych ataków.	K_W06 K_W08 K_W10	laboratorium	Zaliczenie na ocenę	pisemny test lub projekt
U2	potrafi konfigurować wybrane mechanizmy zabezpieczeń sieciowych, takie jak zapory sieciowe, sieci VPN czy zabezpieczenia sieci bezprzewodowych.	K_W06 K_W08 K_W10	laboratorium	Zaliczenie na ocenę	pisemny test lub projekt
U3	potrafi korzystać z narzędzi do monitorowania, analizy i testowania bezpieczeństwa sieci komputerowych.	K_W06 K_W08 K_W10	laboratorium	Zaliczenie na ocenę	pisemny test lub projekt
K1	jest gotów do odpowiedzialnego stosowania zasad bezpieczeństwa w systemach i sieciach komputerowych oraz do ciągłego aktualizowania wiedzy w zakresie nowych zagrożeń i metod ochrony.	K_K01	Wykład/ laboratorium	Zaliczenie na ocenę	Obserwacja, aktywność na zajęciach

Literatura i pomoce naukowe
<p><b>Literatura podstawowa:</b></p> <ol style="list-style-type: none"> <li>1. William Stallings – Network Security Essentials: Applications and Standards, Pearson.</li> <li>2. Charlie Kaufman, Radia Perlman, Mike Speciner – Network Security: Private Communication in a Public World, Prentice Hall.</li> <li>3. William Stallings – Cryptography and Network Security: Principles and Practice, Pearson.</li> </ol> <p><b>Literatura uzupełniająca:</b></p> <ol style="list-style-type: none"> <li>1. Eric Cole – Network Security Bible, Wiley.</li> <li>2. Jon Erickson – Hacking: The Art of Exploitation, No Starch Press.</li> <li>3. Dokumentacja oraz materiały dotyczące narzędzi i technologii bezpieczeństwa sieciowego, takich jak Wireshark, Snort czy OpenVPN.</li> <li>4. Wołoszyn, J. W., &amp; Molga, A. M. (2025). Artificial intelligence in science and technology : from biomedical image analysis to engineering and digital security. W Monografie - Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego (No. 346; s. 113). Uniwersytet Radomski im. Kazimierza Pułaskiego. <a href="https://katalog.uniwersytetradom.pl/1783601774065/woloszyn-jacek/artificial-intelligence-in-science-and-technology?bibFilter=178">https://katalog.uniwersytetradom.pl/1783601774065/woloszyn-jacek/artificial-intelligence-in-science-and-technology?bibFilter=178</a></li> <li>5. Wołoszyn, J. W., &amp; Molga, A. M. (2025). Advanced Artificial Intelligence Methods in Cybersecurity, Threat and Anomaly Detection Using Unsupervised Learning Techniques. Dydaktyka Informatyki , Article 20. <a href="https://doi.org/10.15584/di.2025.20.15">https://doi.org/10.15584/di.2025.20.15</a></li> </ol>

6. Wołoszyn, J. W., & Wołoszyn, M. (2025). Practical Implementation of Artificial Intelligence in Cybersecurity, One-Class SVM for Anomaly Detection in Network Traffic. *Dydaktyka Informatyki*, Article 20. <https://doi.org/10.15584/di.2025.20.17>

Szczegółowy wykaz dodatkowych źródeł i pomocy naukowych na pierwszych zajęciach podaje prowadzący.

Naład 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	60 [h]
Przygotowanie do zajęć, Przygotowanie do zaliczenia	40 [h]	X
Sumaryczne obciążenie pracą studenta	40 [h]/ 1,6 ECTS	60 [h]/ 2,4 ECTS
Punkty ECTS za przedmiot	4 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>