

KARTA PRZEDMIOTU (SYLABUS)

Opis przedmiotu

Kod przedmiotu		Nazwa przedmiotu	BEZPIECZEŃSTWO W SYSTEMACH INFORMATYCZNYCH	
E/O/2/ST/C1B-4B-AII			INFORMATION SYSTEM SECURITY	
Język wykładowy		język polski		
Rok akademicki		2023/2024		
Kierunek		Elektrotechnika		
w zakresie		Automatyka i informatyka		
Poziom studiów		studia drugiego stopnia		
Profil studiów		ogólnoakademicki		
Forma studiów		studia stacjonarne		
Semestr / semestry		3		
Przynależność do grupy zajęć		C1B. Grupa zajęć obieralnych –do wyboru		
Status przedmiotu		obieralny		
Formy realizacji zajęć dydaktycznych, wymiar, punkty ECTS		Forma zajęć	Liczba godzin zajęć dydaktycznych	Liczba punktów ECTS
		Wykład	30 [h]	2 ECTS
		Projekt	15 [h]	
Powiązanie przedmiotu	z profilem studiów	związany z prowadzoną działalnością naukową w dyscyplinach, do których przyporządkowany jest kierunek studiów		0,5 ECTS
	z uprawnieniami	służy do zdobywania przez studenta kompetencji inżynierskich		1 ECTS
	z dyscypliną	automatyka, elektronika, elektrotechnika i technologie kosmiczne		2 ECTS
Forma nauczania		tradycyjna – zajęcia zorganizowane w Uczelni i/lub zajęcia z wykorzystaniem metod i technik kształcenia na odległość (max. 1,2 ECTS)		
Wymagania wstępne		-		
Jednostka prowadząca		Katedra Informatyki i Teleinformatyki		
Koordynator		dr hab. inż. Marcin Chrzan, prof. UTH		
Adres strony internetowej pjo		www.wteii.uniwersytetradom.pl		
Adres e-mail, telefon koordynatora		m.chrzan@uthrad.pl, +48 48 361 77 08		

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

Cel kształcenia:	Celem przedmiotu jest zapoznanie studentów z podstawowymi problemami bezpieczeństwa systemów informatycznych.
Treści programowe:	<p>Wykład [BN, W1]:</p> <ol style="list-style-type: none"> 1. Podstawowe problemy bezpieczeństwa (przestępstwa komputerowe ; polityka bezpieczeństwa; normy i zalecenia klasy bezpieczeństwa systemów komputerowych; podstawowe środki ostrożności i mechanizmy ochrony; mechanizmy uwierzytelniania; uwierzytelnianie biometryczne; strategie autoryzacji i kontroli dostępu (m.in. uznaniowa i ścisła kontrola dostępu, listy ACL); ograniczanie podsłuchu; mechanizmy podnoszenia stopnia dostępności informacji (redundancja komponentów, archiwizacja i kopie zapasowe) 2. Elementy kryptografii (szyfry symetryczne, szyfry asymetryczne; zarządzanie kluczami (PKI); funkcje skrótu i podpis cyfrowy; uwierzytelnianie kryptograficzne; prawne aspekty wykorzystania kryptografii) 3. Bezpieczeństwo systemów operacyjnych (typowe naruszenia bezpieczeństwa; problemy uwierzytelniania i kontroli dostępu współczesnych systemów operacyjnych; wirusy, konie trojańskie i in.; zamaskowane kanały komunikacyjne; ograniczone środowiska wykonania; delegacja uprawnień administracyjnych) 4. Bezpieczeństwo infrastruktury sieciowej (bezpieczeństwo podstawowych protokołów i urządzeń sieciowych w poszczególnych warstwach modelu OSI; narzędzia podnoszące poziom bezpieczeństwa sieci; tunele VPN i protokół IPsec; zapory sieciowe (firewall); bezpieczeństwo infrastruktury sieci bezprzewodowych i urządzeń mobilnych (WiFi, Bluetooth); bezpieczeństwo usług VoIP) 5. Bezpieczeństwo aplikacji użytkowych i usług (bezpieczne środowisko aplikacyjne; problemy ochrony popularnych usług aplikacyjnych: WWW, poczta elektroniczna, komunikatory internetowe; ochrona na poziomie warstwy sesji (protokół SSL/TLS); zagrożenia technologii

	<p>aplikacji internetowych; bezpieczne protokoły aplikacyjne (X.400, PEM, PGP) 3h</p> <p>6. Bezpieczne programowanie (krytyczne błędy programistyczne, np. przepełnienie bufora; ochrona przed błędami; bezpieczna kompilacja; bezpieczne biblioteki; sztuka tworzenia bezpiecznego kodu)</p> <p>7. Środowiska o podwyższonym bezpieczeństwie (interfejs usług bezpieczeństwa; kerberos; GSSAPI; SASL; PAM; bazy danych o podwyższonym bezpieczeństwie)</p> <p>8. Zarządzanie bezpieczeństwem (monitorowanie zabezpieczeń, przynęty i pułapki, kamuflaż, detekcja intruzów (IDS/IPS); narzędzia analizy zabezpieczeń; dzienniki zdarzeń, gromadzenie statystyk, rejestry lokalne i centralne; aktualizacja systemów operacyjnych i aplikacji)</p> <p style="text-align: right;">Suma 30[h]</p> <p>Projekt [BN, U1, K1]: W ramach zajęć studenci wykonują zadanie projektowe dotyczące:</p> <ul style="list-style-type: none"> – modularnych systemów uwierzytelniania i kontroli dostępu do systemu operacyjnego; – ograniczonych środowisk wykonania aplikacji (ograniczone powłoki systemu operacyjnego środowisk serwerowych, delegacja uprawnień administracyjnych); – zabezpieczania usług aplikacyjnych i usług narzędziowych; – systemów programowych i sprzętowych zapór sieciowych (firewall); osobiste zapory (personal firewall); – systemów wykrywania włamań IDS (snort), reakcji na włamania, dokumentowania incydentów. <p style="text-align: right;">Suma 15[h]</p>
Metody dydaktyczne (kształcenia):	<ul style="list-style-type: none"> – metody podające (wykład informacyjny) – metody aktywizujące (metoda przypadków, metoda sytuacyjna, dyskusja dydaktyczna), – metody eksponujące (film, pokaz), – metody programowane (z wykorzystaniem komputera), – metody praktyczne (ćwiczenia laboratoryjne, rachunkowe, symulacja).
Rygor zaliczenia, kryteria oceny osiągniętych efektów uczenia się, sposób obliczania oceny końcowej:	<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. Sposób obliczenia oceny końcowej z przedmiotu określa regulamin studiów. Sposób obliczania oceny z poszczególnych form zajęć przedstawia się następująco:</p> <p>Ocenę z wykładu stanowi wynik egzaminu.</p> <p>Za wykonanie projektu student otrzymuje max 100% pkt., z czego 20% pkt. za prawidłowy tok rozwiązywania zadania, 30% pkt. za prawidłowe określenie jednostek i uzyskany wynik, 50% pkt. za prezentację wyników.</p> <p>Ocena 2 poniżej 50% pkt. Ocena 3 od 51% do 60% pkt. Ocena 3,5 od 61% do 70% pkt. Ocena 4 od 71% do 80% pkt. Ocena 4,5 od 81% do 90% pkt. Ocena 5 powyżej 91% pkt.</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	procedury oraz problemy bezpieczeństwa systemów informatycznych	K_WG06 K_WG08	wykład	egzamin	test otwarty
U1	dobierać odpowiednią metodę ochrony w celu zapewnienia bezpieczeństwa urządzeń i systemów informatycznych projektować bezpieczne systemy informatyczne z uwzględnieniem aspektów prawnych	K_UW02 K_UW08 K_UO15	projekt	zaliczenie z oceną	ocena projektu
K1	świadomego i odpowiedzialnego stosowania procedur bezpieczeństwa w systemach informatycznych	K_KO02	wykład \ projekt	zaliczenie z oceną	aktywność, dyskusja, ocena projektu

Literatura i pomoce naukowe	
1.	D. R. Ahmad, Hack Proofing Your Network, Syngress Publ. 2001.
2.	W. R. Cheswick, Firewalle i bezpieczeństwo w sieci. Helion, 2003.
3.	N. Dhanjani, J. Clarke, Bezpieczeństwo sieci. Narzędzia. Helion 2005.
4.	N. Ferguson, B. Schneier, Kryptografia w praktyce., Helion, 2004
5.	J. Scambray, S. Mc Clure, G. Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill 2000.
6.	M. Schiffman, Hacker's Challenge, Osborne/McGraw-Hill 2001.
7.	J. Stokłosa, T. Bliski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych. PWN, 2001.
8.	M. Strebe, Ch. Perkins, Firewalls. Sybex Inc. 2000.
9.	M. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej. Helion 2005.
10.	William Stallings, Cryptography and Network Security: Principles and Practice, PEARSON EDUC; Edycja 007 (5 marca 2016)
11.	Normy branżowe, zalecenia
12.	W. Stallings, Network Security Essentials. Prentice Hall, 2003.
13.	Smith Sr. Charles L Performing Security Analyses of Information Systems. 1st Book Library. 2018
14.	H. Susanto; M. Nabil Almunawar. Apple Academic Press.2021
15.	D. Kim , M. G. Solomon. Fundamentals of Information Systems Security. Jones & Bartlett Learning. 2021
16.	. Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley John + Sons. 2021

Nakład pracy studenta potrzebny do osiągnięcia zakładanych efektów uczenia się – bilans punktów ECTS			
Udział w zajęciach, aktywność	Obciążenie studenta [h]		
	Inne godz. kontaktowe (IGK)	Zajęcia bez nauczyciela-praca własna studenta (ZBN)	Zajęcia dydaktyczne
Udział w wykładach	X	X	30 [h]
Udział w ćwiczeniach / laboratoriach / projektach / seminariach	X	X	15 [h]
Udział w konsultacjach	3 [h]	X	X
Przygotowanie do wykładów / ćwiczeń / laboratoriów / projektów / seminariów	X	2 [h]	X
Przygotowanie do zaliczenia/egzaminu			
Sumaryczne obciążenie pracą studenta	3 [h] /0,1 ECTS	2 [h] /0,1 ECTS	45 [h] /1,8 ECTS
Punkty ECTS za przedmiot	2 ECTS		

Informacje dodatkowe, uwagi
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. 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.