



3. KARTA PRZEDMIOTU

Kod przedmiotu	Z-ID-U-404
Nazwa przedmiotu	Bezpieczeństwo danych w systemach komputerowych
Nazwa przedmiotu w języku angielskim	Data Security in Computer Systems
Obowiązuje od roku akademickiego	2019/2020

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	INŻYNIERIA DANYCH
Poziom kształcenia	I stopień
Profil studiów	Praktyczny
Forma i tryb prowadzenia studiów	Studia stacjonarne
Zakres	Wszystkie specjalności
Jednostka prowadząca przedmiot	Katedra Informatyki i Matematyki Stosowanej
Koordinator przedmiotu	Dr inż. Zbigniew Sender
Zatwierdził	Dr hab. inż. Artur Bartosik, prof. PŚk

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	Przedmiot kierunkowy
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	Polski
Usytuowanie modułu w planie studiów - semestr	Semestr IV
Wymagania wstępne	Sieci komputerowe i aplikacje sieciowe
Egzamin (TAK/NIE)	TAK
Liczba punktów ECTS	3

Forma prowadzenia zajęć	wykład	ćwiczenia	laboratorium	projekt	inne
Liczba godzin w semestrze	15		15		

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student posiada wiedzę o rodzajach możliwych zagrożeń danych w systemach komputerowych oraz podstawowych metodach zabezpieczeń danych.	ID1_W08 ID1_W07 ID1_W17
	W02	Posiada podstawową wiedzę o metodach szyfrowania danych, podpisie cyfrowym, certyfikatach i aktualnie stosowanych algorytmach szyfrowania.	ID1_W08 ID1_W07 ID1_W09
	W03	Posiada podstawową wiedzę w zakresie bezpiecznych protokołów sieciowych oraz firewalli i usług VPN.	ID1_W08 ID1_W07
Umiejętności	U01	Student potrafi skonfigurować usługi zapewnienia bezpieczeństwa w SO Windows, w tym usług pocztowych.	ID1_U08
	U02	Potrafi zaprogramować podstawowe algorytmy szyfrowania danych.	ID1_U09
	U03	Potrafi zainstalować i wykonać podstawową konfigurację firewalla sieciowego. Potrafi zainstalować i wykonać podstawową konfigurację usługi VPN.	ID1_U08 ID1_U01
Kompetencje społeczne	K01	Student rozumie potrzebę stałego uzupełniania wiedzy z obszaru sieci komputerowych oraz rozumie potrzebę troski o bezpieczeństwo w sieciach komputerowych.	ID1_K01

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. Normy i zalecenia zarządzania bezpieczeństwem danych, rodzaje ataków na systemy informatyczne, ogólne własności bezpieczeństwa danych w systemach Windows.
	2. Elementy kryptografii, algorytmy podstawowych metod szyfrowania.
	3. Elementy kryptografii, programowanie algorytmów podstawowych metod szyfrowania.
	4. Wybrane zagadnienia zabezpieczeń usług sieciowych w środowisku Windows Server. Bezpieczne protokoły sieciowe SSL, IPsec.
	5. Wybrane zagadnienia z zakresu zabezpieczeń w sieciach komputerowych. Firewallle brzegowe sieci komputerowych.
	6. Sieci prywatne – tworzenia bezpiecznych połączeń punkt-punkt (VPN).
	7. Własności koncentratorów sieci VPN.
	8. Zaliczenie – test wielokrotnego wyboru.
laboratorium	1. Konfiguracja zabezpieczeń w komputerze klienta sieci komputerowej w środowisku Windows (przykładowy antywirus i przykładowy firewall).
	2. Programowanie usług szyfrowania danych w wybranym języku programowania (szyfry symetryczny).
	3. Szyfrowania danych w systemach pocztowych.
	4. Konfiguracja zabezpieczeń w serwerze usług sieciowych w środowisku Windows Server.
	5. Konfiguracja firewalla brzegowego sieci komputerowej.
	6. Instalacja i konfiguracja serwera VPN.
	7. Instalacja i konfiguracja klienta VPN.
	8. Zaliczenie – test wielokrotnego wyboru.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia (zaznaczyć X)					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01		X				
W02		X				
W03		X				
U01			X		X	
U02			X		X	
U03			X		X	
K01					X	

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	egzamin	Uzyskanie co najmniej 50% punktów z pracy pisemnej oraz z testu.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z oceny sprawozdań z wykonania laboratorium w trakcie zajęć oraz z testu.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS							
Lp.	Rodzaj aktywności	Obciążenie studenta					Jednostka
		W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	15		15			h
2.	Inne (konsultacje, egzamin)	2		2			h
3.	Razem przy bezpośrednim udziale nauczyciela akademickiego	34					h
4.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	1,4					ECTS
5.	Liczba godzin samodzielnej pracy studenta	41					h
6.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	1,6					ECTS
7.	Nakład pracy związany z zajęciami o charakterze praktycznym	38					h
8.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1,5					ECTS
9.	Sumaryczne obciążenie pracą studenta	75					h
10.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	3					ECTS

LITERATURA

1. Chałon M., *Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2007.
2. Serafin M., *Sieci VPN: zdalna praca i bezpieczeństwo danych*, Helion, Gliwice 2008.
3. Stokłosa J, Bilski T, Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Wydaw. Naukowe PW-N, Warszawa 2001.