KARTA PRZEDMIOTU

Nazwa przedmiotu: ***Praktyczna administracja siecią (TIAu>SM2-PAS-19-O)***
Nazwa w języku polskim:
Nazwa w jęz. angielskim: ***The practice of network administration***

Dane dotyczące przedmiotu:

Jednostka oferująca przedmiot: Wydział Automatyki, Elektroniki i Informatyki
Przedmiot dla jednostki: Politechnika Śląska

Domyślny typ protokołu dla przedmiotu:

ZAL

Język wykładowy:

polski

Strona WWW:

https://platforma.polsl.pl/rau2/course/view.php?id=1127

Skrócony opis:

Celem przedmiotu jest przedstawienie praktycznych aspektów związanych z zabezpieczaniem i administrowaniem sieci komputerowych. Studenci posiądą wiedzę praktyczną oraz teoretyczną dotyczącą działania urządzeń, systemów sieciowych oraz mechanizmów ochrony powszechnie stosowanych. Zapoznają się z metodami zabezpieczania dostępu oraz potencjalnymi zagrożeniami.
Przedmiot ten jest przaznaczony przede wszystkim dla osób chcących zrozumieć i zarządzać bezpiecznie swoją siecią lokalną oraz tych, którzy chcą zostać w przyszłości administratorami sieci.

Opis:

Wykład:
Sieci komputerowe są wykorzystywane dziś w praktycznie wsystkich dziedzinach życia. Większość społeczeństwa posiada dostęp do internetu i w dużej mierze nie jest świadoma zagrożeń, które powstają w momencie podpięcia do „sieci”.
Przedmiot ma na celu zaznajomienie słuchaczy z praktycznymi aspektami zabezpieczania i przeciwdziałania nieuprawnionemu dostępowi do sieci. Pozwoli zrozumieć potrzeby wykorzystania autoryzacji do sieci bezprzewodowej, jak i przewodowej. Przedstawione zostaną mechanizmy wykorzystywane przez dostawców internetu na styku z klientem końcowym. Metody zabezpieczeń dostępu oraz jego słabe punkty. Główny nacisk zostanie położony na praktyczne zastosowanie zdobytej wiedzy.
Laboratorium:
1. Mechanizmy zdalnego dostępu.
2. Wirtualne sieci prywatne.
3. Zabezpieczanie dostępu w sieciach bezprzewodowych.
4. Enkapsulacja pakietów (PPPoE).

Liczba godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów
Liczba punktów ECTS:2
Całkowita liczba godzin: 60 (kontaktowo 30h / praca własna 30h)
Wykład: 10 godzin
Laboratorium: 20 godzin
Praca własna studenta; przygotowanie do laboratorium i opracowanie rezultatów

Literatura:

Kizza M. J.: Guide To Computer Network Security, Springer 2020
Serafin M.: Sieci VPN. Zdalna praca i bezpieczeństwo danych, Helion, 2010

Efekty uczenia się:

Ma wiedze z zakresu nowoczesnej konfiguracji końcowej infrastruktury sieciowej. - K2A_W09, K2A_U05, K2A_U14
Ma wiedzę na temat nowoczesnych zabezpieczeń transmisji w sieci.- K2A_W09, K2A_U14
Zna współczesne typy zagrożeń sieciowych, metody ich wykrywania i zapobiegania.- K2A_W09, K2A_U03
Zna mechanizmy zabezpieczeń dostępu do sieci. - K2A_W09, K2A_U01

Metody i kryteria oceniania:

sprawozdanie z ćwiczenia laboratoryjnego lub wykonanie prezentacji lub aktywność na zajęciach.

Sylabus obowiązuje od roku akademickiego 2021/2022, a jego zawartość nie podlega zmianom w trakcie trwania semestru

Punkty przedmiotu w cyklach:

<bez przypisanego programu>

Typ punktów	Liczba	Cykl pocz.	Cykl kon.
Europejski System Transferu Punktów (ECTS)	2	2021/2022-Z	