



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo urządzeń sieciowych [S2Teleinf2-STRC>BU]

Przedmiot

Kierunek studiów

Teleinformatyka

Rok/Semestr

1/2

Studia w zakresie (specjalność)

Sieci teleinformatyczne i rozwiązania chmurowe

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład

14

Laboratorium

24

Inne (np. online)

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

3,00

Koordynatorzy

dr hab. inż. Piotr Zwierzykowski prof. PP

piotr.zwierzykowski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający przedmiot powinien posiadać wiedzę dotyczącą budowy i działania sieci komputerowych. W szczególności powinien znać podstawowe protokoły zapewniające komunikację w sieci (ARP, IPv4/IPv6, RIP, DHCP). Powinien również posiadać podstawą wiedzę z zakresu rachunku prawdopodobieństwa i probablistyki. Student powinien posiadać także podstawie umiejętności z zakresu obsługi systemu operacyjnego linux.

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z zagadnieniami związanymi z bezpieczeństwem urządzeń sieciowych. W ramach przedmiotu poruszane są tematy związane z urządzeniami IoT, przemysłowymi jak również z zarządzaniami sieciami klasy operatorskiej i dostępowej.

Przedmiotowe efekty uczenia się

Wiedza:

Ma poszerzoną i pogłębioną wiedzę w zakresie bezpieczeństwa urządzeń wchodzących w skład firmowych i przemysłowych sieci teleinformatycznych [K2_W02].

Zna i rozumie algorytmy wykorzystywane w systemach teleinformatycznych [K2_W05].

Umiejętności:

Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie [K2_U01].

Potrafi zaplanować oraz przeprowadzić eksperymenty badawcze, w tym: testowanie, symulację, pomiary charakterystyk, ekstrakcję parametrów, analizę i syntezę bezpiecznych systemów teleinformatycznych [K2_U07].

Kompetencje społeczne:

Jest gotów do odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych, w tym: rozwijania dorobku zawodu, podtrzymywania etosu zawodu, przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad (K2_K06).

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta w ramach wykładu weryfikowana jest przez zaliczenie w formie pisemnej lub ustnej. W formie pisemnej studenci muszą udzielić odpowiedzi na 6 pytań (testowych i otwartych) różnie punktowanych. Są trzy grupy punktowe (1,2 i 3 punkty). Natomiast w przypadku egzaminu ustnego student losuje po dwa pytania z każdej grupy punktowej. W formie ustnej, do każdego wylosowanego pytania, student może otrzymać dodatkowe pytanie (związane z wylosowanym pytaniem). Ocena pytania (obejmuje odpowiedź zarówno na pytanie wylosowane jak i pytanie dodatkowe) obejmuje zakres odpowiedzi oraz głębię zrozumienia zagadnienia. Do każdego egzaminu przygotowywanych jest 60 pytań. Warunkiem pozytywnego zaliczenia egzaminu otrzymanie minimum 50% punktów możliwych do zdobycia.

Kryteria oceny egzaminu i zaliczania:

liczba punktów ocena

≤ 6 punktów 2,0

7-8 punktów 3,0

9 punktów 3,5

10 punktów 4,0

11 punktów 4,5

12 punktów 5,0

Umiejętności nabyte w ramach laboratorium weryfikowane są na podstawie zadań realizowanych w trakcie trwania zajęć. Za każde zadanie student otrzymuje ocenę. Ocena końcowa jest średnią ze wszystkich ocen, przy czym konieczne jest, aby wszystkie zadania otrzymały ocenę pozytywną.

Treści programowe

Przedmiot obejmuje przedstawienie i omówienie obszarów zapewniania bezpieczeństwa urządzeń sieciowych w sieciach teleinformatycznych.

Tematyka zajęć

1. Przedstawienie i omówienie obszarów zapewniania bezpieczeństwa urządzeń sieciowych
2. Zabezpieczenie ruterów i przełączników pracujących w firmowych sieciach IP
3. Bezpieczny zdalny dostęp do urządzeń sieciowych (VPN, AAA)
4. Urządzenia zapewniające bezpieczny dostęp do urządzeń sieciowych i końcowych (zapory sieciowe)
5. Bezpieczeństwo łańcuchów dostaw
6. Bezpieczeństwo urządzeń IoT
7. Ataki wykorzystujące rekonensans i sposoby zabezpieczania się przed nimi.
8. Analiza bezpieczeństwa funkcjonalnego rozwiązań sieciowych

Metody dydaktyczne

Wykłady: w zależności od omawianego tematu oraz od zainteresowania studentów wykład prowadzony jest w jednej z trzech form: wykład tradycyjny (prezentacja multimedialna uzupełniona przykładami podawanymi na tablicy), wykład problemowy (dyskusja ze słuchaczami nad rozwiązaniem danego problemu), lub wykład konwersatoryjny (wciąganie słuchaczy w dyskusję, sterowanie przebiegiem wykładu w zależności od udzielanych odpowiedzi itp.).

Ćwiczenia laboratoryjne: ćwiczenia prowadzone są w laboratorium Akademii Sieci Huawei lub Cisco. W trakcie zajęć studenci wykonują zadania przedstawione przez prowadzącego, które polegają na odpowiednim połączeniu urządzeń (przełączniki, routery i komputery) i konfiguracji urządzeń sieciowych zgodnie z wymaganiami danego ćwiczenia.

Literatura

Podstawowa:

1. Marek Serafin: Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone, Helion, 2013
2. Marvin Rausand, Reliability of Safety-Critical Systems: Theory and Applications, John Wiley & Sons, 2014

Uzupełniająca:

1. Omar Santos: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, 2020

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	78	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	40	1,50