Karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE PODSTAWOWE

Nazwa zajęć: Protokoły i technologie bezpieczeństwa sieciowego	Cykl kształcenia rozpoczynający się w roku akademickim: 2023/24
Nazwa kierunku studiów, poziom i profil kształcenia: informatyka, studia I-go stopnia, inżynierskie	
Język wykładowy: polski	Rodzaj zajęć: zajęcia specjalistyczne
Rok studiów: III	Semestr: VI
Liczba punktów ECTS przypisana zajęciom: 4	Koordynator zajęć Imię, nazwisko, tytuł/stopień naukowy, adres e-mail:
Jednostka organizacyjna: Instytut Inżynierii Technicznej, Zakład Informatyki	

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN

Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:

Studia stacjonarne		**Studia niestacjonarne**	
Wykład:	15	Wykład:	
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:	30	Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki zawodowe:		Praktyki zawodowe:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:	45	**RAZEM:**	

II. INFORMACJE SZCZEGÓŁOWE

Wymagania wstępne i dodatkowe:studenci powinni posiadać elementarną wiedzę z zakresu technologii sieciowych, teorii głównych protokołów TCP/IP, umiejętność zarządzania serwerowymi systemami operacyjnymi i systemami urządzeń sieciowych, a także umiejętność instalacji i konfiguracji podstawowych usług sieciowych

Cel (cele) kształcenia dla zajęć:zdobycie przez studentów wiedzy dotyczącej elementarnych zasad prowadzenia polityki bezpieczeństwa sieciowego, teorii wybranych protokołów bezpieczeństwa, a także zdobycie umiejętności wdrażania stosownych technologii, implementowanych w systemach urządzeń sieciowych oraz w systemach serwerowych.

EFEKTY UCZENIA SIĘ OKREŚLONE DLA ZAJĘĆ I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ OKREŚLONYCH DLA KIERUNKU STUDIÓW		
Efekty uczenia się określone dla zajęć w kategorii wiedza, umiejętności oraz kompetencje społeczne oraz metody weryfikacji efektów uczenia się		
Symbol efektów uczenia się określonego dla zajęć	Treść efektu uczenia się. Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się określonych dla kierunku studiów (symbol efektów uczenia się)
Wiedzy - zna i rozumie		
W_01	elementarne pojęcia związane z kreowaniem polityki bezpieczeństwa sieciowego przedsiębiorstwa,	K_W07, K_W20
W_02	mechanizmy wybranych protokołów bezpieczeństwa	K_W07
Umiejętności - potrafi		
U_01	dobrać odpowiednie technologie bezpieczeństwa stosownie do potrzeb	K_U07, K_U10, K_U13, K_U16
U_02	wdrożyć i konfigurować wybrane usługi bezpieczeństwa, implementowane w serwerowych systemach operacyjnych oraz w urządzeniach sieciowych	K_U07, K_U10, K_U16
Kompetencji społecznych - jest gotów do		
K_01	ma świadomość konieczności podnoszenia swoich kwalifikacji poprzez samokształcenie, ze względu na dynamiczny rozwój technologii	K_K01

TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO FORM ZAJĘĆ I METOD OCENIANIA			
Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć, tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):			
Symbol treści programowych	Opis treści programowych	Metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć
wykład			

TP-01	Podstawowe zagadnienia z zakresu zarządzania bezpieczeństwem sieci: definicje poziomów polityki bezpieczeństwa, domeny informacyjne przedsiębiorstwa, ogólna charakterystyka zagrożeń i ich form. Rodzaje przestępstw komputerowych: kradzież haseł, socjotechnika, błędy, niepowodzenia uwierzytelnienia, wypływ informacji, ataki sieciowe. Strefa bezpieczeństwa sieciowego – charakterystyka elementów strefy. Wybrane aspekty bezpieczeństwa energetycznego.	Wykład podający, wykład problemowy, pogadanka	Egzamin pisemny i ustny
TP-02	Problematyka bezpiecznego, zdalnego zarządzania infrastrukturą sieciową - mechanizmy protokołu SSH. Wybrane protokoły bezpieczeństwa implementowane w urządzeniach sieciowych: port security, protokół 802.1x-RADIUS, spanning-tree-protocol.	Wykład podający, wykład problemowy, pogadanka	Egzamin pisemny i ustny
TP-03	Scenariusze wybranych ataków sieciowych: ataki DOS, techniki penetracji systemów, rekonesans, określenie słabych punktów i wybór celów, zdobycie kontroli nad systemem. Sprzętowe zapory sieciowe - funkcje podstawowe i uboczne zapór.	Wykład podający, wykład problemowy, pogadanka	Egzamin pisemny i ustny
TP-04	Infrastruktura klucza publicznego PKI, rola urzędów certyfikacji. Aspekty techniczne wdrażania protokołu TLS/SSL w usłudze WWW.	Wykład podający, wykład problemowy, pogadanka	Egzamin pisemny i ustny
zajęcia praktyczne			
TP-05	Wprowadzenie do przedmiotu: ogólna charakterystyka merytoryczna ćwiczeń praktycznych, przewidzianych do realizacji, zasady BHP obowiązujące w laboratorium.	pogadanka	weryfikacja poprawności realizacji ćwiczeń praktycznych

TP-06	Wdrażanie protokołu *SSH* w systemie serwerowym GNU/Linux, MS Windows Serwer oraz w systemie *Cisco IOS*. Wykorzystanie protokołu *SFTP*. Wdrażanie certyfikatów SSH.	realizacja ćwiczeń praktycznych z wykorzystaniem stacji sieciowych, maszyn wirtualnych oraz urządzeń sieciowych (przełączniki, routery)	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
TP-07	Wdrażanie protokołu *Kerberos* do mechanizmów *SSH* oraz NFS w systemie *GNU*/*Linux*.	realizacja ćwiczeń praktycznych z wykorzystaniem stacji sieciowych, maszyn wirtualnych	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
TP-08	Badanie protokołu *port-security* w przełącznikach Cisco.	realizacja ćwiczeń praktycznych z wykorzystaniem urządzeń sieciowych - przełączniki warstwy 2	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
TP-09	Badanie mechanizmów połączeń nadmiarowych (protokół STP)	realizacja ćwiczeń praktycznych z wykorzystaniem urządzeń sieciowych - przełączniki warstwy 2	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
TP-10	Konfiguracja mechanizmów autentykacji i autoryzacji w sieci LAN za pomocą protokołu *RADIUS* (system GNU/Linux i Windows Server. Wykorzystanie certyfikatów serwera w mechanizmach protokołu.	realizacja ćwiczeń praktycznych z wykorzystaniem stacji sieciowych, maszyn wirtualnych oraz urządzeń sieciowych (przełączniki)	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
TP-11	Bezpieczeństwo systemu *DNS* - wdrożenie protokołu *DNSSEC* w systemie *Windows Server*	realizacja ćwiczeń praktycznych z wykorzystaniem stacji sieciowych oraz maszyn wirtualnych	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
TP-12	Badanie funkcji podstawowych i ubocznych sprzętowej zapory sieciowej Juniper SRX 320	realizacja ćwiczeń praktycznych z wykorzystaniem stacji sieciowych oraz urządzeń sieciowych Juniper SRX 320	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
ZALECANA LITERATURA (w tym pozycje w języku obcym)			

Literatura podstawowa:

1. McNab Ch.: *Ocena bezpieczeństwa sieci wyd. 3,*wyd. APNPromise 2017r.

2. Fry. C., Nystrom M.: Monitoring i bezpieczeństwo sieci, wyd.Helion 2010r.

3. Dokumentacja techniczna Juniper SRX 320

4. oficjalny serwis: *www.openssh.com*

5. oficjalny serwis: *www.openssl.org*

6. oficjalny serwis: *freeradius.org*

Literatura uzupełniająca:

1. Olejnik Ł. Kurasiński A.: Filozofia cyberbezpieczeństwa PWN Warszawa 2022

2. *ComputerWorld*- aktualne wydania czasopisma

III. INFORMACJE DODATKOWE

BILANS PUNKTÓW ECTS

OBCIĄŻENIE PRACĄ STUDENTA (godziny)

Forma aktywności	Liczba godzin
Godziny zajęć (według harmonogramu) z nauczycielem akademickim lub inną osobą prowadzącą zajęcia	45
Praca własna studenta	50
SUMA GODZIN:	95

OBCIĄŻENIE PRACĄ STUDENTA (punkty ECTS)

		Liczba punktów ECTS	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPISANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim lub inną osobą prowadzącą zajęcia	Ogółem: 4	2
	Praca własna studenta		2

OPIS PRACY WŁASNEJ STUDENTA:

Czytanie wskazanej literatury

1) technologie SSH, TLS.SSL, RADIUS (W_01, W_02, U_01, U_02) - ocena wykonywanych ćwiczeń praktycznych, egzamin

Przygotowanie do wykonania ćwiczeń praktycznych

1) Ugruntowanie wiedzy z zakresu teorii systemu DNS W_02, U_01, U_02 ocena wykonywanych ćwiczeń praktycznych

2) Znajomość administrowania systemami sieciowymi Windows Server (Power Shell) oraz GNU Linux (cli)

W_01, W_02, U_01, U_02, ocena wykonywanych ćwiczeń praktycznych

3) Ugruntowanie wiedzy z zakresu teorii protokołu Kerberos oraz NFS (W_01, W_02, U_01, U_02), ocena wykonywanych ćwiczeń praktycznych

Przygotowanie do egzaminu

1) znajomość podstaw teoretycznych kluczowych protokołów bezpieczeństwa sieciowego (W_01, W_02), egzamin

KRYTERIA OCENIANIA

Ocena kształtująca: podjęta będzie na podstawie zajęć praktycznych, które kończą się zaliczeniem na ocenę Warunkiem uzyskania oceny pozytywnej z zajęć praktycznych jest realizacja wszystkich przewidzianych ćwiczeń:

- na ocenę dostateczną student wykorzystuje w stopniu podstawowym zdobytą wiedzę i umiejętności praktyczne do realizacji zaplanowanym ćwiczeń z pomocą prowadzącego zajęcia

- na ocenę dobrą student wykorzystuje w stopniu zadowalającym zdobytą wiedzę i umiejętności praktyczne do samodzielnej realizacji zaplanowanych ćwiczeń

- na ocenę bardzo dobrą student samodzielnie zdobywa i wykorzystuje wiedzę oraz umiejętności praktyczne biegle posługując się wszystkimi podstawowymi i zaawansowanymi aspektami przedmiotu. Przedstawia własne koncepcje rozwiązania problemów.

Ocena podsumowująca: zajęcia kończą się egzaminem. Warunkiem przystąpienia do egzaminu jest pozytywna ocena z zajęć praktycznych. Przewiduje się egzamin pisemny i ustny.

INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA KSZTAŁCENIA NA ODLEGŁOŚĆ