Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE

Nazwa zajęć: protokoły i technologie bezpieczeństwa sieciowego	Cykl kształcenia: 2021/22	Data aktualizacji sylabusa:
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: 3	Koordynator zajęć Imię, nazwisko, tytuł/stopień naukowy, adres e-mail: dr Robert Pękala, robert.pekala@pwste.edu.pl	
Jednostka organizacyjna: Instytut Inżynierii Technicznej, Zakład Informatyki	Prowadzący zajęcia dr Robert Pękala, robert.pekala@pwste.edu.pl mgr inż. Marek Zarychta, marek.zarychta@pwste.edu.pl	

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:		Praktyki:	
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	
Symbol efektów uczenia się określonego dla zajęć	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
W_01	elementarne pojęcia związane z kreowaniem polityki bezpieczeństwa sieciowego przedsiębiorstwa,
W_02	mechanizmy wybranych protokołów bezpieczeństwa
Umiejętności - potrafi	
U_01	dobrać odpowiednie technologie bezpieczeństwa stosownie do potrzeb
U_02	wdrożyć i konfigurować wybrane usługi bezpieczeństwa, implementowane w serwerowych systemach operacyjnych oraz w urządzeniach sieciowych
Kompetencji społecznych - jest gotów do	
K_01	ma świadomość konieczności podnoszenia swoich kwalifikacji poprzez samokształcenie, ze względu na dynamiczny rozwój technologii
K_02	posiada świadomość konieczności stosowania technologii bezpieczeństwa w infrastrukturze sieciowej LAN firmy lub instytucji

TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ OKREŚLONYCH DLA ZAJĘĆ

Symbol treści programowych	Opis treści programowych	Liczba godzin	Odniesienie do 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.	3	W_01, K_02

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.	4	W_01, W_02
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.	4	W_01, W_02
TP-04	Infrastruktura klucza publicznego PKI, rola urzędów certyfikacji. Aspekty techniczne wdrażania protokołu TLS/SSL w usłudze WWW.	4	W_01, W_02
zajęcia praktyczne			
TP-05	Wprowadzenie do przedmiotu: ogólna charakterystyka merytoryczna ćwiczeń praktycznych, przewidzianych do realizacji, zasady BHP obowiązujące w laboratorium.	2	W_01, W_02, K_01
TP-06	Wdrażanie protokołu *SSH* w systemie serwerowym GNU/Linux, MS WIndows Serwer oraz w systemie *Cisco IOS*. Wykorzystanie protokołu *SFTP*. Konfiguracja protokołu z dwoma parami kluczy.	6	W_02, U_02, K_02
TP-07	Wdrażanie protokołu *Kerberos* do mechanizmów *SSH* oraz NFS w systemie *GNU/Linux*.	2	W_02, U_01, U_02, K_01, K_01, K_02
TP-08	Badanie protokołu *port-security* w przełącznikach Cisco.	2	W_01, W_02, U_01, U_02, K_01, K_02
TP-09	Badanie mechanizmów połączeń nadmiarowych (protokół STP)	2	W_01, W_02, U_01, U_02, K_01, K_02
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.	4	W_01, W_02, U_01, U_02, K_01, K_02
TP-11	Bezpieczeństwo systemu *DNS* - wdrożenie protokołu *DNSSEC* w systemie *Windows Server*	4	W_02, U_01, U_02, K_01, K_02
TP-12	Badanie funkcji podstawowych i ubocznych sprzętowej zapory sieciowej Juniper SRX 320	4	W_01, W_02, U_01, U_02, K_01, K_02

TP-13	Wdrażanie protokołu *TLS*/*SSL* w systemach serwerowych Windows Server oraz *GNU*/*Linux*. Wykorzystanie certyfikatów lokalnego oraz publicznego *CA*.	4	W_02, U_01, U_02, K_01, K_02

ZALECANA LITERATURA (w tym pozycje w języku obcym)

Literatura podstawowa:

1. *McNab Ch.: Ocena bezpieczeństwa sieci wyd. 3,* wyd. APN Promise 2017r.
2. Dokumentacja techniczna Juniper SRX 320
3. oficjalny serwis: *www.openssh.com*
4. oficjalny serwis: *www.openssl.org*
5. oficjalny serwis: *freeradius.org*

Literatura uzupełniająca:

1. *ComputerWorld* - aktualne wydania czasopisma
2. Ramon J.*: Bezpieczeństwo systemu Linux*, MIKOM, Warszawa 2002r.

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się określonych dla zajęć i treści programowych do form zajęć i metod oceniania

Symbol efektu uczenia się określonego dla zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągniecie założonych efektów uczenia się	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć
Wiedza			
W_01	TP-01, TP-02, TP-03, TP-04	Wykład podający, wykład problemowy, pogadanka	egzamin pisemny
W_02	TP-02, TP-03, TP-04	Wykład podający, wykład problemowy, pogadanka	egzamin pisemny
Umiejętności			
U_01	TP-10, TP-12, TP-13	realizacja ćwiczeń praktycznych,	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia
U_02	TP-06÷TP-13	realizacja ćwiczeń praktycznych,	weryfikacja poprawności realizacji ćwiczeń praktycznych, krótkie zaliczenie pisemne przed realizacją ćwiczenia

Kompetencje społeczne			
K_01	TP-14	pogadanka związana z teoretycznymi treściami merytorycznymi w odniesieniu do ćwiczeń praktycznych,	obserwacja aktywności studentów na zajęciach, zaliczenie pisemne ćwiczeń
K_02	TP-02, TP-06÷TP-13	pogadanka związana z teoretycznymi treściami merytorycznymi w odniesieniu do ćwiczeń praktycznych,	obserwacja aktywności studentów na zajęciach, zaliczenie pisemne ćwiczeń

BILANS PUNKTÓW ECTS	
OBCIĄŻENIE PRACĄ STUDENTA (godziny)	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (według harmonogramu) z nauczycielem	45
Praca własna studenta: czytanie wskazanej literatury, przygotowanie do zajęć praktycznych przygotowanie do egzaminu	40
SUMA GODZIN:	**85**

OBCIĄŻENIE PRACĄ STUDENTA (punkty ECTS)			
		Liczba punktów ECTS	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPISANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	3	1.6
	Praca własna studenta		1.4

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
Zajęcia praktyczne kończą się zaliczeniem na ocenę, zaś przedmiot kończy się egzaminem. Przewiduje się egzamin pisemny. Warunkiem uzyskania oceny pozytywnej z zajęć praktycznych jest realizacja wszystkich przewidzianych ćwiczeń. Kryteria oceniania zajęć praktycznych: - 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 zaplanowanym - 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.
INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA B-LEARNINGU nie przewiduje się
INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU Istnieje możliwość wykorzystania metody e-learningu do realizacji treści zajęć wykładowych

(data, podpis Koordynatora odpowiedzialnego za zajęcia)**:**

…….. …….
(imię i nazwisko) (podpis i data)

Podpis kierownika zakładu:

…….. …….
(imię i nazwisko) (podpis i data)

Podpis dyrektora instytutu:

…….. …….
(imię i nazwisko) (podpis i data)