



IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	E-1IZ4T-05-S8
Nazwa przedmiotu	Zaawansowane techniki bezpieczeństwa sieci teleinformatycznych
Nazwa przedmiotu w języku angielskim	Advanced in Teleinformatic Network Security
Obowiązuje od roku akademickiego	2019/20

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	
Poziom kształcenia	
Profil studiów	
Forma i tryb prowadzenia studiów	
Zakres	
Jednostka prowadząca przedmiot	
Koordynator przedmiotu	dr inż. Radosław Belka dr inż. Justyna Kęczkowska
Zatwierdził	Dziekan Wydziału Elektrotechniki Automatyki i Informatyki Dr hab. inż. Antoni Różowicz, prof. PŚk

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	
Status przedmiotu	
Język prowadzenia zajęć	
Usytuowanie modułu w planie studiów - semestr	
Wymagania wstępne	Sieci Komputerowe; Podstawy routingu i przełączania; Cyberbezpieczeństwo
Egzamin (TAK/NIE)	
Liczba punktów ECTS	

Forma prowadzenia zajęć	wykład	ćwiczenia	laboratorium	projekt	Inne
Liczba godzin w semestrze	9	0	18	18	0

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W27	zna ryzyka związane z naruszeniem bądź brakiem bezpieczeństwa systemów informatycznych, w tym z niewłaściwą ochroną danych osobowych, ma uporządkowaną wiedzę na temat metod zapobiegania im	INF1_W27
	W28	zna mechanizmy zabezpieczania zasobów systemu informatycznego przed nieuprawnionym użyciem	INF1_W28
Umiejętności	U04	potrafi przygotować i przedstawić krótką prezentację poświęconą wynikom realizacji zadania inżynierskiego	INF1_U04
	U31	Potrafi stosować techniki wspomagające bezpieczeństwo systemów komputerowych.	INF1_U31
	U32	rozumie znaczenie sprawnego komunikowania się z osobami, z którymi pracuje w zespole.	INF1_U32
Kompetencje społeczne	K07	rozumie i docenia społeczny kontekst informatyki i związane z nim ryzyko oraz potrzebę oceny sytuacji pojawiających się w życiu zawodowym informatyka, zarówno pod względem prawnym, jak i etycznym	INF1_K07

TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
Wykład	1. Sieci komputerowe i teleinformatyczne – powtórzenie. Architektura sieci komputerowych
	2. Klasyfikacja zagrożeń sieci w sieciach teleinformatycznych Świadomość zagrożeń. Typy i metody ataków sieciowych. Polityka bezpieczeństwa.
	3. Zabezpieczanie urządzeń sieciowych na przykładzie routerów i przełączników Cisco. Definiowanie poziomów uprzywilejowania oraz RoleBased CLI.
	4. Aspekty wykorzystania modelu AAA w polityce bezpieczeństwa. Protokoły autentykacji Radius, Tacacs+, Kerberos.
	5. Konceptcje Firewall. Zaawansowane metody implementacji ACL. ACL dynamiczne, refleksywne, czasowe. Kontrola CBAC (Content-Based Access Control) . Statefull Firewalls. Konceptcje Zone Based Policy Firewall (ZBPF)
	6. Systemy detekcji i prewencji – IDS, IPS.
	7. Lokalne sieci komputerowe - przegląd protokołów w aspekcie zagrożeń. Zabezpieczanie sieci lokalnych w standardzie Ethernet.
	8. Konceptcje VPN, site-site i remote. Protokoły kryptograficzne wykorzystywane w VPN. IPSec, IKE i ISAKMP.
	9. Zapoznanie się z platformą ASA 5500. Konfiguracja funkcji firewall oraz VPN ASA 5505.
	10. Podsumowanie i powtórzenie materiału. Test kontrolny
laboratorium	1. Podstawowe procedury przy zabezpieczaniu urządzeń. Konfiguracja SSH
	2. Konfiguracja ARP access list jako metoda przeciwdziałania zagrożeniom typu IP spoofing
	3. Konfiguracja funkcji DHCP snooping
	4. Konfiguracja funkcji Dynamic ARP Ispection
	5. Zabezpieczenia przeciwko atakom na protokół STP i atakom typu broadcast storm.
	6. Zabezpieczanie protokołów routingu dynamicznego - funkcje uwierzytelniające
	7. Poziomy uprzywilejowania - definiowanie widoków i superwidoków
	8. Konfiguracja rozszerzonych list kontroli dostępu (extended ACL)

	9. Konfiguracja Content Based Access Control (CBAC) i funkcji inspec
	10. Konfiguracja ZBPF
	11. Obsługa IDS/IPS
	12. Konfiguracja VPN na routerach Cisco
	13. Konfiguracja sprzętowych firewali ASA 5500
	14. Podsumowanie - ćwiczenie integrujące wiadomości

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W27			X	X	X	
W28			X	X	X	X
U04			X	X	X	X
U31			X	X	X	X
U32			X	X	X	X
K07			X	X	X	X

A.

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia	Warunki zaliczenia
wykład		Uzyskanie co najmniej 50% punktów z testu egzaminacyjnego
laboratorium		Wykonanie wszystkich zaplanowanych ćwiczeń laboratoryjnych, uzyskanie co najmniej 50 % punktów z kolokwium zaliczeniowego
projekt	zaliczenie z oceną	Opracowanie i obrona projektu zespołowego, sporządzenie raportu końcowego

*) zostawić tylko realizowane formy zajęć

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS							
Lp.	Rodzaj aktywności	Obciążenie studenta					Jednostka
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	h
		9		18	18		
3.	Inne (konsultacje, egzamin)*	2		2	2		h
4.	Razem przy bezpośrednim udziale nauczyciela akademickiego	51					h
5.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	2,04					ECTS
6.	Liczba godzin samodzielnej pracy studenta	99					h
7.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	3,96					ECTS

8.	Nakład pracy związany z zajęciami o charakterze praktycznym	42	h
9.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1,65	ECTS
10.	Sumaryczne godzinowe obciążenie pracą studenta	150	h
11.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	6	

** wszelkie formy weryfikacji efektów, w tym egzaminy oraz nie więcej niż 2 godziny konsultacji dla każdej formy zajęć*

LITERATURA

1. Libor Dostalek, Bezpieczeństwo protokołu TCP/IP kompletny przewodnik, wyd. MIKOM PWN
2. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, wyd. Helion
3. E. Schetina, K. Green, J. Carlson, Bezpieczeństwo w sieci, wyd. Helion
4. Materiały firmy Cisco – instrukcje routerów i przełączników Cisco.
5. A. Józefiok, Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco”, Helion 2016