Załącznik nr 7
do Zarządzenia Rektora nr 10/12
z dnia 21 lutego 2012r.

KARTA MODUŁU / KARTA PRZEDMIOTU

Kod modułu	
Nazwa modułu	**Zaawansowane techniki bezpieczeństwa sieci teleinformatycznych**
Nazwa modułu w języku angielskim	**Advanced in Teleinformatic Network Security**
Obowiązuje od roku akademickiego	**2018/2019**

A. USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**I stopień**
Profil studiów	**ogólnoakademicki**
Forma i tryb prowadzenia studiów	**stacjonarne**
Specjalność	**Teleinformatyka**
Jednostka prowadząca moduł	**Zakład Fotoniki i Systemów Teleinformatycznych**
Koordynator modułu	**Dr inż. Radosław Belka**
Zatwierdził:	**Dziekan WEAiI** **dr hab. inż. Antoni Różowicz, prof. PŚk**

B. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	**przedmiot specjalnościowy**
Status modułu	**obieralny**
Język prowadzenia zajęć	**Polski**
Usytuowanie modułu w planie studiów - semestr	**semestr VII**
Usytuowanie realizacji przedmiotu w roku akademickim	**semestr zimowy**
Wymagania wstępne	**Sieci Komputerowe;** **Podstawy routingu i przełączania;** **Cyberbezpieczeństwo**
Egzamin	**tak**
Liczba punktów ECTS	**7**

Forma prowadzenia zajęć	**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Godzin w semestrze	**15**		**30**	**30**	

C. EFEKTY KSZTAŁCENIA I METODY SPRAWDZANIA EFEKTÓW KSZTAŁCENIA

Cel modułu	Celem modułu jest zdobycie zaawansowanej wiedzy na temat zagrożeń i bezpieczeństwa sieci teleinformatycznych oraz umiejętności z zakresu zabezpieczania urządzeń sieciowych i konfiguracji zabezpieczeń protokołów sieciowych w sieciach teleinformatycznych

Symbol efektu	Efekty kształcenia	Forma prowadzenia zajęć *(w/ć/l/p/inne)*	odniesienie do efektów kierunkowych	odniesienie do efektów obszarowych
W_01	Ma wiedzę na temat zagrożeń bezpieczeństwa w sieciach teleinformatycznych i wynikających z tego konsekwencji	W/L	K_W10 K_W17	T2A_W02 T2A_W04
W_02	Zna zaawansowane systemy i procedury zabezpieczeń stosowane w sieciach teleinformatycznych	W/L	K_W10	T2A_W04 T2A_W05
W_03	Zna procedury kryptograficzne stosowane w bezpiecznej komunikacji w sieciach teleinformatycznych	W/L	K_W10	T2A_W04
U_01	Potrafi dokonać krytycznej analizy sposobu funkcjonowania sieci teleinformatycznej pod kątem ich bezpieczeństwa.	W/L	K_U01 K_U02 K_U16	T2A_U01 T2A_U08 T2A_U12
U_02	Potrafi przeprowadzić podstawową konfigurację zabezpieczeń urządzeń sieciowych (routery, przełączniki, firewalle) oraz poprawnie zaimplementować rozwiązania VPN	W/L	K_U01 K_U02 K_U16	T2A_U08 T2A_U16
U_03	Potrafi wybrać najlepsze w danej sytuacji rozwiązanie sprzętowe i programowe.	W/L	K_U01 K_U02 K_U16	T2A_U01 T2A_U16
.....				
K_01	Ma świadomość podstawowych zagrożeń w sieciach teleinformatycznych (podsłuchu, utraty lub modyfikacji danych) i ich wpływu na społeczeństwo	W/L	K_K01 K_K01	T2A-K01 T2A-K02
K_02	Potrafi pracować i współdziałać w grupie w zakresie projektowania i konfiguracji bezpiecznej sieci	L	K_K01 K_K01	T2A-K01 T2A-K02
.....				

Treści kształcenia:

1. Treści kształcenia w zakresie wykładu

Nr wykładu	Treści kształcenia	Odniesienie do efektów kształcenia dla modułu
1.	Sieci komputerowe i teleinformatyczne – powtórzenie. Architektura sieci komputerowych	W_01
2-3	Klasyfikacja zagrożeń sieci w sieciach teleinformatycznych Świadomość zagrożeń. Typy i metody ataków sieciowych. Polityka bezpieczeństwa.	W_01 K_01 U_01
4	Zabezpieczanie urządzeń sieciowych na przykładzie routerów i przełączników Cisco. Definiowanie poziomów uprzywilejowania oraz Role-Based CLI.	W_03 U_01
5	Aspekty wykorzystania modelu AAA w polityce bezpieczeństwa. Protokoły autentykacji Radius, Tacacs+, Kerberos.	W_01 U_02
6-7	Koncepcje Firewall. Zaawansowane metody implementacji ACL. ACL dynamiczne, refleksywne, czasowe. Kontrola CBAC (Content-Based Access Control) . Statefull Firewalls. Koncepcje Zone Based Policy Firewall (ZBPF)	W_01; W_02 U_01
8	Systemy detekcji i prewencji – IDS, IPS.	W_01 U_02; U_03
9-10.	Lokalne sieci komputerowe - przegląd protokołów w aspekcie zagrożeń. Zabezpieczanie sieci lokalnych w standardzie Ethernet.	W_01; W_02 U_01
11-12	Koncepcje VPN, site-site i remote. Protokoły kryptograficzne wykorzystywane w VPN. IPSec, IKE i ISAKMP.	W_01; W_03 U_02; U_03
13-14	Zapoznanie się z platformą ASA 5500. Konfiguracja funkcji firewall oraz VPN ASA 5505.	W_01; W_02 U_02
15	Podsumowanie i powtórzenie materiału. Test kontrolny	W_01; W_02 U_01; U_02

2. Treści kształcenia w zakresie ćwiczeń – **nie dotyczy**

3. Treści kształcenia w zakresie zadań laboratoryjnych

Nr zajęć lab.	Treści kształcenia	Odniesienie do efektów kształcenia dla modułu
1	Podstawowe procedury przy zabezpieczaniu urządzeń. Konfiguracja SSH	W_01; W_02 U_01; U_02 K_01
2	Konfiguracja ARP access list jako metoda przeciwdziałania zagrożeniom typu IP spoofing	W_01; W_02 U_01; U_02 K_01; K_02
3	Konfiguracja funkcji DHCP snooping	W_01; W_02 U_01; U_02 K_02
4	Konfiguracja funkcji Dynamic ARP Ispection	W_01; W_02 U_01; U_02 K_02
5	Zabezpieczenia przeciwko atakom na protokół STP i atakom typu broadcast storm.	W_01 W_02 U_01; U_02 K_02
6	Zabezpieczanie protokołów routingu dynamicznego - funkcje uwierzytelniające	W_01; W_02 U_01; U_02 K_01; K_02
7	Poziomy uprzywilejowania - definiowanie widoków i superwidoków	W_01; W_02 U_01; U_02 K_02
8	Konfiguracja rozszerzonych list kontroli dostępu (extended ACL)	W_01; W_02 W_03 U_01; U_02

		K_01; K_02
9	Konfiguracja Content Based Access Control (CBAC) i funkcji inspec	**W_01; W_02** **U_01; U_02** **K_01; K_02**
10	Konfiguracja ZBPF	**W_01; W_02** **U_01; U_02** **K_01; K_02**
11	Obsługa IDS/IPS	**W_01; W_02** **W_03** **U_01; U_02** **K_01; K_02**
12	Konfiguracja VPN na routerach Cisco	**W_01; W_02** **W_03** **U_01; U_02** **K_01; K_02**
13-14	Konfiguracja sprzętowych firewalli ASA 5500	**W_01; W_02** **W_03** **U_01; U_02** **K_01; K_02**
15	Podsumowanie - ćwiczenie integrujące wiadomości	**W_01; W_02** **W_03** **U_01; U_02** **K_01**

4. Charakterystyka zadań projektowych

1. Grupowy (2-3 osoby) projekt demonstracyjnej sieci komputerowej z zaimplementowanymi wybranymi rozwiązaniami polityki bezpieczeństwa, zrealizowanej przy użyciu modeli urządzeń i protokołów sieciowych z wykorzystaniem programów symulacyjnych takich jak Cisco Packet Tracer oraz GNS3.
2. Przygotowanie skryptów konfiguracyjnych dla urządzeń w postaci plików tekstowych
3. Przetestowanie implementacji na urządzeniach rzeczywistych – demonstracja w warunkach zbliżonych do rzeczywistych
4. Sporządzenie opracowania końcowego - raportu
5. Obrona projektu

Metody sprawdzania efektów kształcenia

Symbol efektu	**Metody sprawdzania efektów kształcenia** *(sposób sprawdzenia, w tym dla umiejętności – odwołanie do konkretnych zadań projektowych, laboratoryjnych, itp.)*
W_01	Egzamin z wiedzy teoretycznej
W_02	Zadania praktyczne – konfiguracja zabezpieczeń
W_03	Test wiedzy teoretycznej
U_01	Egzamin z wiedzy teoretycznej
U_02	Egzamin z wiedzy teoretycznej, realizacja ćwiczeń laboratoryjnych
U_03	Realizacja ćwiczeń laboratoryjnych
K_01	Test wiedzy teoretycznej
K_02	Realizacja ćwiczeń praktycznych – praca w grupach.

D. NAKŁAD PRACY STUDENTA

Bilans punktów ECTS	
Rodzaj aktywności	**obciążenie studenta**
Udział w wykładach	**15g**
Udział w ćwiczeniach	
Udział w laboratoriach	**30g**
Udział w konsultacjach (2-3 razy w semestrze)	**5g**
Udział w zajęciach projektowych	**30g**
Konsultacje projektowe	**8g**
Udział w egzaminie	**2g**
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela akademickiego	**90g** *(suma)*
Liczba punktów ECTS, którą student uzyskuje na zajęciach wymagających bezpośredniego udziału nauczyciela akademickiego *(1 punkt ECTS=25-30 godzin obciążenia studenta)*	**3.6**
Samodzielne studiowanie tematyki wykładów	**10g**
Samodzielne przygotowanie się do ćwiczeń	
Samodzielne przygotowanie się do kolokwiów	**10g**
Samodzielne przygotowanie się do laboratoriów	**10g**
Wykonanie sprawozdań	**15g**
Przygotowanie do kolokwium końcowego z laboratorium	**5g**
Wykonanie projektu lub dokumentacji	**25g**
Przygotowanie do egzaminu	**10g**
Liczba godzin samodzielnej pracy studenta	**85g** *(suma)*
Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy *(1 punkt ECTS=25-30 godzin obciążenia studenta)*	**3.4**
Sumaryczne obciążenie pracą studenta	**175g**
Punkty ECTS za moduł *1 punkt ECTS=25-30 godzin obciążenia studenta*	**7**

E. LITERATURA

Wykaz literatury	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 ruterów i przełączników Cisco. 5. A. Józefiok, Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco", Helion 2016
Witryna WWW modułu/przedmiotu	www.netacad.com