Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-02-s2
	studia niestacjonarne:	E-1IZ2C-1002-s2
Nazwa przedmiotu	**Bezpieczeństwo infrastruktury sieciowej**	
Nazwa przedmiotu w języku angielskim	**Network security**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**dr inż. Mirosław PŁAZA, mgr inż. Michał Zawadzki**
Zatwierdził	**Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**Przedmiot specjalnościowy**
Status przedmiotu		**Obowiązkowy**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr II**
	studia niestacjonarne	**Semestr II**
Wymagania wstępne		**brak**
Egzamin (TAK/NIE)		**TAK**
Liczba punktów ECTS		**5**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**			**30**	
	studia niestacjonarne:	**18**			**18**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie zagrożenia związane z bezpieczeństwem infrastruktury sieciowej.	INF2_W02
	W02	Student zna i rozumie podstawowe technologie zabezpieczeń stosowane w infrastrukturze sieciowej.	INF2_W02
	W03	Student zna i rozumie struktury rozwiązań bezpieczeństwa implementowanych w infrastrukturze sieciowej.	INF2_W02
Umiejętności	U01	Student potrafi konfigurować podstawowe zabezpieczenia infrastruktury sieciowej.	INF2_U02, INF2_U09
	U02	Student potrafi przewidywać ataki na infrastrukturę sieciową i odpowiednio im zapobiegać.	INF2_U01, INF2_U05
	U03	Student potrafi weryfikować poziom bezpieczeństwa infrastruktury sieciowej.	INF2_U02, INF_U09
Kompetencje społeczne	K01	Student jest gotów do poszerzania kompetencji w zakresie zagrożeń związanych z bezpieczeństwem infrastruktury sieciowej.	INF2_K03 INF2_K04
	K02	Student jest gotów do pracy i współdziałania w grupie w zakresie implementacji podstawowych technologii związanych z bezpieczeństwem infrastruktury sieciowej.	INF2_K03 INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Infrastruktura klucza publicznego** (weryfikacja tożsamości, wymiana kluczy kryptograficznych, wystawianie i weryfikacja certyfikatów, podpisywanie i szyfrowanie przekazu, potwierdzanie tożsamości, znakowanie czasem). 2. **Zabezpieczanie urządzeń sieciowych na przykładzie routerów i przełączników** (zabezpieczenie dostępu do urządzeń, poziomy uprawnień, bezpieczna konfiguracja Syslog/SNMP/NTP). 3. **Uwierzytelnianie, autoryzacja i rozliczanie** (modele uwierzytelniania, protokoły autentykacji Radius, Tacacs+, Kerberos). 4. **Zaawansowane metody implementacji ACL** (ACL dynamiczne, refleksywne, czasowe). **5. Zagrożenia bezpieczeństwa sieci w warstwie 2** (przepełnienie tablic adresowych przełącznika - ataki typu MAC *flooding*, nadużycia w implementacjach VLAN, wykorzystanie protokołu ARP, ataki z wykorzystaniem protokołu Spanning Tree, inne typy ataków na L2) 6. **Zabezpieczanie STP** (BPDU Guard, BPDU Filtering, Root Guard, Loop Guard) 7. **Koncepcje zapory (firewall)** (w wariancie bezstanowym i stanowym, filtracja a inspekcja pakietów, koncepcje stanowego firewall opartego na strefach / ZBPF - Zone Based Policy Firewall). 8. **Wybrane zagadnienia z zakresów automatycznych systemów detekcji i prewencji** (IDS, NIDS, HIDS, IPS). 9. **Zaawansowane rozwiązania bezpieczeństwa w obszarze sieci VLAN oraz sieci bezprzewodowych**.

projekt	Tematyka zadań projektowych z zakresu Bezpieczeństwa infrastruktury sieciowej obejmuje następujące zagadnienia: analizę literatury w zakresie dotychczas stosowanych rozwiązań dotyczących zadanego problemu inżynierskiego; analizę oraz dobranie odpowiednich technik umożliwiających skuteczną realizację zadanego problemu wraz z uzasadnieniem dokonanych wyborów; projekt opracowywanego systemu/zadania wraz z opisem zastosowanych technik oraz narzędzi; przygotowanie dokumentacji projektowej, która w sposób szczegółowy opisuje wykonany projekt wraz z założeniami projektowymi – dokumentacja przygotowywana jest samodzielnie przez zespół realizujący projekt; opis sposobu implementacji opracowanego rozwiązania wraz z instrukcją obsługi; analizę dalszych możliwości rozwoju przygotowanego rozwiązania, prezentacja opracowanego rozwiązania.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01		X				
W02		X				
W03		X				
U01		X		X		
U02		X		X		
U03		X		X		
K01				X		
K02				X		

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	egzamin	Uzyskanie co najmniej 50% punktów z egzaminu.
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z wykonanego projektu.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30			**30**		**18**			**18**		
2.	Inne (konsultacje, egzamin)	**4**			**2**		**4**			**2**		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**66**					**42**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,64**					**1,68**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**59**					**83**					h

6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**2,36**	**3,32**	ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**	**18**	h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,2**	**0,72**	ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**125**	**125**	h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**5**		ECTS

LITERATURA

1. Omar Santos, **CCNA Security - Official Cert Guide**, 2015
2. Kibet John, **Best CCNA Security Certification Study Book**, 2022
3. Glen D. Singh, Michael Vinod, Vijay Anandh,**CCNA Security Certification Guide**, 2019