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

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	
	studia niestacjonarne:	
Nazwa przedmiotu	**Zaawansowane techniki bezpieczeństwa sieci tele-informatycznych**	
Nazwa przedmiotu w języku angielskim	**Advanced network security**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**I stopień**
Profil studiów	**ogólnoakademicki**
Forma i tryb prowadzenia studiów	**studia stacjonarne i niestacjonarne**
Zakres	**Teleinformatyka**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**dr inż. Radosław Belka**
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		**wybieralny**
Język prowadzenia zajęć		**polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**semestr VII**
	studia niestacjonarne	**semestr VIII**
Wymagania wstępne		**Sieci komputerowe, Podstawy routingu i przełączania, Sieci korporacyjne**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**6**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**		**15**	**30**	
	studia niestacjonarne:	**18**		**9**	**18**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie problematykę zagrożeń bezpieczeństwa w sieciach teleinformatycznych.	INF1_W32
	W02	Student zna i rozumie działanie zaawansowanych systemów i procedur zabezpieczeń stosowanych w sieciach teleinformatycznych.	INF1_W32
	W03	Student zna i rozumie procedury kryptograficzne stosowane w bezpiecznej komunikacji w sieciach teleinformatycznych	INF1_W32
Umiejętności	U01	Student potrafi przeprowadzić konfigurację urządzeń sieciowych oraz poprawnie zaimplementować zaawansowane rozwiązania bezpieczeństwa.	INF1_U32
	U02	Student potrafi dokonać krytycznej analizy sposobu funkcjonowania sieci teleinformatycznej pod kątem bezpieczeństwa.	INF1_U32
	U03	Student potrafi wybrać najlepsze w danej sytuacji rozwiązanie sprzętowe i programowe.	INF1_U32
Kompetencje społeczne	K01	Student jest gotów do podjęcia działalności w zakresie uświadamiania zagrożeń sieci i definiowania polityki bezpieczeństwa	INF1_K01 INF1_K02
	K02	Student jest gotów pracować w współdziałać w grupie w zakresie obejmującym projektowanie i konfigurowanie bezpiecznej sieci teleinformatycznej.	INF1_K01 INF1_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. Zabezpieczanie urządzeń sieciowych jako ważny element bezpieczeństwa systemów teleinformatycznych. Zabezpieczenie dostępu do urządzeń. Poziomy i domeny uprawnień dostępu do urządzeń sieciowych. 2. Protokoły monitorowania i nadzorowania sieci jako element bezpieczeństwa. 3. Uwierzytelnianie, autoryzacja i rozliczanie – model AAA. Protokoły wspomagające dla modelu AAA. 4. Koncepcje zapory (firewall) w wariancie bezstanowym i stanowym. Filtracja a inspekcja pakietów. Koncepcje stanowego firewall opartego na strefach (ZBPF - Zone Based Policy Firewall). 5. Wybrane zagadnienia z zakresów automatycznych systemów detekcji i prewencji (IDS, IPS). 6. Bezpieczeństwo warstwy łącza danych i warstwy sieciowej- zagrożenia i sposoby przeciwdziałania. 7. Podstawowe protokoły i techniki kryptograficzne w zastosowaniach VPN i IPSec *8.* Zarządzanie bezpieczną siecią. Polityka bezpieczeństwa i projektowanie bezpiecznych sieci. Weryfikacja bezpieczeństwa sieci.
laboratorium	1. Podstawowe procedury stosowane przy zabezpieczaniu urządzeń. Poziomy uprzywilejowania - definiowanie widoków i superwidoków. 2. Konfiguracja zabezpieczeń przeciwko zagrożeniom w sieciach LAN 3. Konfiguracja zabezpieczeń przeciwko zagrożeniom typu IP spoofing. 4. Zabezpieczanie protokołów routingu dynamicznego. 5. Rozszerzone listy kontroli dostępu – konfiguracja. 6. Konfiguracja funkcji firewall zgodnie z koncepcją Zone-Based Policy. 7. Obsługa systemu detekcji i prewencji intruzów (IDS/IPS). 8. Zaawansowana konfiguracja VPN. 9. Konfiguracja sprzętowa firewalli

Projekt	Grupowy (2-3 osoby) projekt sieci korporacyjnych z zaimplementowanymi mechanizmami zabezpieczeń. Projekt wymaga zintegrowania wcześniej poznanych technologii sieciowych z zakresu routingu i przełączania z metodami zabezpieczeń sieci LAN, obsługą firewall oraz konfiguracją bezpiecznych tuneli przez segment publiczny. Projekt wymaga dokonania wyboru środowiska pracy, dobór technologii sieciowych i protokołów, wybór urządzeń i ich konfiguracja, testowanie oraz sporządzenie dokumentacji

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

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

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z zaliczenia
laboratorium	zaliczenie z oceną	1. Realizacja warsztatowa wszystkich zalecanych ćwiczeń laboratoryjnych. 2. Pozytywne zaliczenie zadań projektowych integrujących wiadomości (co najmniej 50%)
projekt	Wybierz element.	1. Poprawna realizacja projektu. 2. Poprawna obrona projektu

NAKŁAD PRACY STUDENTA

<table>
<tr><th colspan="13">Bilans punktów ECTS</th></tr>
<tr><th rowspan="3">Lp.</th><th rowspan="3">Rodzaj aktywności</th><th colspan="10">Obciążenie studenta</th><th>Jed-nostka</th></tr>
<tr><th colspan="5">studia stacjonarne</th><th colspan="5">studia niestacjonarne</th><th></th></tr>
<tr><th>W</th><th>C</th><th>L</th><th>P</th><th>S</th><th>W</th><th>C</th><th>L</th><th>P</th><th>S</th><th rowspan="2">h</th></tr>
<tr><td>1.</td><td>Udział w zajęciach zgodnie z planem studiów</td><td>30</td><td></td><td>15</td><td>30</td><td></td><td>18</td><td></td><td>9</td><td>18</td><td></td></tr>
<tr><td>2.</td><td>Inne (konsultacje, egzamin)</td><td>2</td><td></td><td>1</td><td>2</td><td></td><td>2</td><td></td><td>1</td><td>2</td><td></td><td>h</td></tr>
<tr><td>3.</td><td>Razem przy bezpośrednim udziale nauczyciela akademickiego</td><td colspan="5">80</td><td colspan="5">50</td><td>h</td></tr>
<tr><td>4.</td><td>Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego</td><td colspan="5">3,2</td><td colspan="5">2</td><td>ECTS</td></tr>
<tr><td>5.</td><td>Liczba godzin samodzielnej pracy studenta</td><td colspan="5">70</td><td colspan="5">100</td><td>h</td></tr>
<tr><td>6.</td><td>Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy</td><td colspan="5">2.8</td><td colspan="5">4</td><td>ECTS</td></tr>
<tr><td>7.</td><td>Nakład pracy związany z zajęciami o charakterze praktycznym</td><td colspan="5">45</td><td colspan="5">27</td><td>h</td></tr>
<tr><td>8.</td><td>Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym</td><td colspan="5">1,80</td><td colspan="5">1,08</td><td>ECTS</td></tr>
<tr><td>9.</td><td>Sumaryczne obciążenie pracą studenta</td><td colspan="5">150</td><td colspan="5">150</td><td>h</td></tr>
<tr><td>10.</td><td>Punkty ECTS za moduł
1 punkt ECTS=25 godzin obciążenia studenta</td><td colspan="10">6</td><td>ECTS</td></tr>
</table>

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
4. Materiały platformy NetACad udostępniane studentom podczas zajęć.