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	**Wybrane aspekty cyberbezpieczeństwa**	
Nazwa przedmiotu w języku angielskim	**Selected aspects of cybersecurity**	
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	**Systemy informacyjne**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**dr inż. Mirosław PŁAZA**
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**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**6**

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

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie współczesne problemy cyberbezpieczeństwa.	INF1_W32
	W02	Student zna i rozumie rozwiązania pozwalającą zaprojektować / uruchomić usługi bezpieczeństwa w sieci teleinformatycznej.	INF1_W32
	W03	Student zna i rozumie rozwiązania z zakresu architektury, organizacji i bezpieczeństwa systemów operacyjnych.	INF1_W32
Umiejętności	U01	Student potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony przed zagrożeniami.	INF1_U32
	U02	Student potrafi zaprojektować / uruchomić / przetestować usługę bezpieczeństwa w sieci teleinformatycznej.	INF1_U32
	U03	Student potrafi planować i przeprowadzać eksperymenty z zakresu ochrony zasobów dostępnych przez sieci teleinformatyczne.	INF1_U32
Kompetencje społeczne	K01	Student jest gotów do oceny znaczenia cyberbezpieczeństwa w dzisiejszym świecie.	INF1_K01 INF1_K02
	K02	Student jest gotów do pracy i współdziałania w grupie w zakresie obejmującym tworzenie zabezpieczeń w obszarze teleinformatyki.	INF1_K01 INF1_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Wprowadzenie do zagadnień cyberbezpieczeństwa** (cyberprzestrzeń, cyberprzestępczość; rodzaje podatności). 2. **Zagrożenia, luki i ataki w cyberświecie** (oprogramowanie złośliwe i zaawansowane mechanizmy ochrony; ataki DoS, DDoS i sposoby reagowania na nie). 3. **Wybrane rodzaje ataków** (ataki dostępowe; ataki na infrastrukturę i usługi sieciowe; ataki na sieci bezprzewodowe). 4. **Systemy zapobiegające kradzieżom danych.** 5. **Chmury obliczeniowe** (podstawowe rozwiązania z zakresu cyberbezpieczeństwa funkcjonujące w chmurze obliczeniowej). 6. **Projektowanie systemów bezpieczeństwa** (zasady projektowania systemów zabezpieczeń i ich oceny; polityka bezpieczeństwa systemów informatycznych). 7. **Wybrane aspekty prawne w obszarze cyberbezpieczeństwa.** 8. **Zagadnienia cyberbezpieczeństwa w rozwiązaniach IoT** (ocena podatności i ryzyka w systemach IoT, problemy bezpieczeństwa w poszczególnych warstwach modelu odniesienia systemów IoT). 9. **Wybrane kwestie bezpieczeństwa w systemach operacyjnych** (Windows, Linux)
laboratorium	1. Ochrona danych w cyberświecie - badanie integralności danych. 2. Bezpieczeństwo maszyn wirtualnych. 3. Wykrywanie zagrożeń i luk w zabezpieczeniach teleinformatycznych. 4. Ataki na urządzenia stacjonarne oraz mobilne. 5. Badanie ruchu pomiędzy klientem a witryną zdalną. 6. Podstawowa konfiguracja tunelu VPN. 7. Odzyskiwanie haseł użytkownika przy pomocy narzędzi systemowych. 8. Badanie i podstawowa konfiguracja zapory firewall. 9. List kontroli dostępu w zagadnieniach cyberbezpieczeństwa. 10. Ceberbezpieczeństwo IoT - badanie i analiza podatności aplikacji i urządzeń IoT. 11. Bezpieczeństwo w systemów operacyjnych.

projekt	Tematyka zadań projektowych obejmuje: • analizę literatury w zakresie dotychczas stosowanych rozwiązań dotyczących zadanego problemu inżynierskiego, • analiza 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 • analiza dalszych możliwości rozwoju przygotowanego rozwiązania, • prezentacja opracowanego rozwiązania.

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			
U02			X			
U03			X			
K01			X			
K02			X			

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwiów.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwiów.
projekt	zaliczenie z oceną	Obrona przygotowanych projektów

NAKŁAD PRACY STUDENTA

<table>
<tr><th colspan="13">Bilans punktów ECTS</th></tr>
<tr><td rowspan="3">Lp.</td><td rowspan="3">Rodzaj aktywności</td><td colspan="10">Obciążenie studenta</td><td rowspan="3">Jed-nostka</td></tr>
<tr><td colspan="5">studia stacjonarne</td><td colspan="5">studia niestacjonarne</td></tr>
<tr><td>W</td><td>C</td><td>L</td><td>P</td><td>S</td><td>W</td><td>C</td><td>L</td><td>P</td><td>S</td></tr>
<tr><td>1.</td><td>Udział w zajęciach zgodnie z planem studiów</td><td>30</td><td></td><td>30</td><td>15</td><td></td><td>18</td><td></td><td>18</td><td>9</td><td></td><td>h</td></tr>
<tr><td>2.</td><td>Inne (konsultacje, egzamin)</td><td colspan="5">2</td><td colspan="5">2</td><td>h</td></tr>
<tr><td>3.</td><td>Razem przy bezpośrednim udziale nauczyciela akademickiego</td><td colspan="5">81</td><td colspan="5">51</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">3,24</td><td colspan="5">2,04</td><td>ECTS</td></tr>
<tr><td>5.</td><td>Liczba godzin samodzielnej pracy studenta</td><td colspan="5">69</td><td colspan="5">99</td><td>h</td></tr>
<tr><td>6.</td><td>Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy</td><td colspan="5">2,76</td><td colspan="5">3,96</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. Charles J. Brooks, Donald Short, Christopher Grow, **Cybersecurity Essentials**, 2018
2. Omar Santos, **Cisco CyberOps Associate Official Cert Guide**, 2020
3. Cisco Networking Academy, **CCNA Cybersecurity Operations Companion Guide**, 2018