KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: **PODSTAWY CYBERBEZPIECZEŃSTWA**		*Kod przedmiotu:* **KNS/BW-IP/K/34b**
Nazwa przedmiotu w języku angielskim: **CYBER SECURITY BASICS**		
Kierunek studiów: **Bezpieczeństwo wewnętrzne**	*Profil:* **praktyczny**	*Poziom studiów:* **I stopień**
Specjalność/specjalizacja: **-**	*Forma zaliczenia przedmiotu:* **zaliczenie na ocenę**	*Semestr studiów:* **3**
Nazwa grupy zajęć: **zajęcia kierunkowe**	*Język w jakim prowadzone są zajęcia:* **polski**	

Tryb studiów	*Forma zajęć*							*Ogólna liczba godzin*	*Liczba punktów ECTS:*
	W	*Ćw.*	*Konw.*	*Lab.*	*Proj.*	*Sem.*	*Zajęcia terenowe*		
Tryb stacjonarny		**-**	**-**	**15**	**-**	**-**	**-**	**15**	**2**
Tryb niestacjonarny		**-**	**-**	**15**	**-**	**-**	**-**	**15**	

Jednostka realizująca przedmiot, wydział:
Kolegium Nauk Społecznych

Odpowiedzialny za opracowanie karty przedmiotu (tytuł/stopień naukowy, imię i nazwisko, adres e-mail):
dr. inż. Paweł Matuszczyk, pmatuszczyk@wszop.edu.pl

CEL PRZEDMIOTU

C1.	Zapoznanie studentów z podstawowymi pojęciami związanymi z cyberbezpieczeństwem.
C2.	Zapoznanie studentów z zagrożeniami płynącymi z użytkowania sieci lokalnej oraz Internet, a także aplikacji i systemów operacyjnych.

WYMAGANIA WSTĘPNE

1.	Podstawowa wiedza z zakresu technologii informacyjnej.
2.	Podstawowa wiedza z zakresu bezpieczeństwa informacji.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ		METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ	ODNIESIENIE DO:	
			TREŚCI PROGRAMOWYCH	KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ
EU1	Student zna i rozumie współczesne problemy cyberbezpieczeństwa; dysponuje wiedzą pozwalającą zaprojektować i uruchomić usługi bezpieczeństwa w sieci teleinformatycznej	test jednokrotnego wyboru (pytania zamknięte) test - pytania zamknięte i otwarte	L1;L2;L3;L4;L5	BW KW_06
EU2	Student potrafi analizować i wykorzystywać uzyskaną wiedzę do identyfikacji i klasyfikacji napotkanych zagrożeń w cyberprzestrzeni a także podejmować działania mające na celu eliminację lub zmniejszenie ryzyka wystąpienia zagrożeń w cyberprzestrzeni.	test jednokrotnego wyboru (pytania zamknięte) test jednokrotnego wyboru (pytania zamknięte)	L2;L3;L4	BW KU_02
EU3	Student ma świadomość wpływu cyfryzacji na społeczeństwo oraz zagrożeń jakie nowe technologie generują, jest gotów do podnoszenia swoich kwalifikacji; potrafi aktywnie uczestniczyć w dyskusji poświęconej zagadnieniom cyberbepieczeństwa.	test jednokrotnego wyboru (pytania zamknięte)	L1;L2;L3;L4;L5	BW KU_05 BW KK_01

TREŚCI PROGRAMOWE

L.p.	LABORATORIUM	Liczba godzin	
		S	N
L1	Źródła prawa w zakresie ochrony cyberprzestrzeni. Wprowadzenie do zagadnień cyberbezpieczeństwa: cyberprzestrzeń, cyberbezpieczeństwo, cyberprzestępczość.	2	2
L2	Zagrożenia, luki i ataki w cyber świecie – oprogramowanie złośliwe i zawansowane mechanizmy ochrony. Ataki dostępowe. Ataki na infrastrukturę i usługi sieciowe.	5	3
L3	Algorytmy szyfrowania i kontrola dostępu. Elementy kryptografii: kryptografia: symetryczna i asymetryczna.	5	3
L4	Bezpieczeństwo sieci bezprzewodowych. Sieci VPN. Systemy szyfrowania, uwierzytelniania i infrastruktura klucza publicznego (PKI). Maskowanie ataków. Analiza włamań. Systemy zapobiegające wyciekom danych (DLP)	6	4
L5	Systemy IPS/IDS. Rozwiązania w chmurze z zakresu cyberbzpieczeństwa dla małych i średnich przedsiębiorstw.	3	3
	RAZEM	21	15

FORMA I KRYTERIA ZALICZENIA LABORATORIUM: test - pytania zamknięte i otwarte - ocena ilościowa

METODY I FORMY DYDAKTYCZNE	
1.	studium przypadków
2.	wykład problemowy
3.	dyskusja
4.	Ćwiczenia laboratoryjne
NARZĘDZIA DYDAKTYCZNE	
1.	platforma e-learningowa
2.	prezentacja multimedialna
OPROGRAMOWANIE	
1.	Zarządzanie komputerami ITManager

2.	Google Cloud Security Command Center
3.	Azure Security Center

OBCIĄŻENIE STUDENTA PRACĄ

	Forma aktywności	**Liczba godzin na zrealizowanie aktywności**	
		tryb stacjonarny	*tryb niestacjonarny*
1.	godziny kontaktowe z nauczycielem akademickim	**15**	**15**
2.	samodzielne przygotowanie się do zajęć	7	7
3.	przygotowanie do zaliczenia/egzaminu	7	7
4.	konsultacje	3	3
5.	zapoznanie się z literaturą	18	18
6.	zaliczenie/egzamin	-	-
	SUMA GODZIN	**50**	**50**
	LICZBA PUNKTÓW ECTS	**2**	**2**

LITERATURA PODSTAWOWA

1.	Bravo C., *Cyberbezpieczestwo dla zaawansowanych Skuteczne zabezpieczenia systemu Windows Linux IoT i infrastruktury w chmurze,* Helion, Gliwice 2023
2.	Ignatowicz l., *Cyfrowe ślady mówią. Poradnik ochrony prywatności,* Warszawa 2015

LITERATURA UZUPEŁNIAJĄCA I ŹRÓDŁA PRAWA

1.	Lizut J. (red.) *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, Warszawa 2014
2.	Dera P., *Sieci peer to peer – programy klienckie i możliwości identyfikacji ich użytkowania w badaniach kryminalistycznych*, Katowice 2009
3.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa **(**tj. Dz.U. z 2024, poz. 1077)
4.	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz.UE.L Nr 194, str. 1)
5.	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) z dnia 14 września 2022 r. (Dz. Urz. UE. L Nr 265, s. 1)
6.	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE. L Nr 277, s. 1)

INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE:

1.	PLATFORMA MOODLE zawiera: ▪ materiały dydaktyczne do przedmiotu ▪ przedmiotowe efekty uczenia się ▪ zalecaną literaturę ▪ warunki i kryteria zaliczenia przedmiotu
2.	BIBLIOTEKA WSZOP zapewnia literaturę podstawową do przedmiotu oraz wybrane pozycje literatury uzupełniającej, w tym dostęp do zbiorów cyfrowych i Platformy IBUK Libra
3.	ELEKTRONICZNY NIEZBĘDNIK STUDENTA zawiera: ▪ kierunkowe efekty uczenia się ▪ karty przedmiotów ▪ terminy konsultacji nauczycieli akademickich
4.	WIRTUALNY DZIEKANAT zawiera: ▪ harmonogram zajęć na bieżący semestr ▪ harmonogram sesji egzaminacyjnej ▪ ogłoszenia dotyczące organizacji roku akademickiego

5.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny jakościowej oznacza, że zakładane efekty zostały osiągnięte: ▪ w pełni – ocena bardzo dobry ▪ z niewielkimi niedociągnięciami – ocena dobry plus ▪ z brakami, które można uzupełnić – ocena dobry ▪ z istotnymi brakami, które można uzupełnić – ocena dostateczny plus ▪ z istotnymi brakami na minimalnym poziomie – ocena dostateczny lub ▪ nie zostały osiągnięte – ocena niedostateczny.
6.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny ilościowej oznacza, że zakładane efekty zostały osiągnięte: ▪ 91-100% sumy – ocena bardzo dobry ▪ 81-90% – ocena dobry plus ▪ 71-80% – ocena dobry ▪ 61-70% – ocena dostateczny plus ▪ 51-60% – ocena dostateczny lub ▪ 50% i mniej – ocena niedostateczny.
7.	Terminy egzaminów uzgadnia starosta roku z prowadzącym zajęcia
8.	Karta przedmiotu obowiązuje od roku akademickiego 2024/25