

KARTA PRZEDMIOTU

<i>Nazwa przedmiotu w języku polskim:</i> BEZPIECZEŃSTWO SYSTEMÓW OPERACYJNYCH		<i>Kod przedmiotu:</i> KNS/BW-IIP/BC/54							
<i>Nazwa przedmiotu w języku angielskim:</i> OPERATING SYSTEMS SECURITY									
<i>Kierunek studiów:</i> Bezpieczeństwo wewnętrzne	<i>Profil:</i> praktyczny	<i>Poziom studiów:</i> II stopień							
<i>Specjalność/specjalizacja:</i> Bezpieczeństwo cyberprzestrzeni	<i>Forma zaliczenia przedmiotu:</i> egzamin	<i>Semestr studiów:</i> 3							
<i>Nazwa grupy zajęć:</i> zajęcia specjalnościowe	<i>Język w jakim prowadzone są zajęcia:</i> polski								
<i>Tryb studiów</i>	<i>Forma zajęć</i>							<i>Ogólna liczba godzin</i>	<i>Liczba punktów ECTS:</i>
	<i>W</i>	<i>Ćw.</i>	<i>Konw.</i>	<i>Lab.</i>	<i>Proj.</i>	<i>Sem.</i>	<i>Zajęcia terenowe</i>		
<i>Tryb stacjonarny</i>	15		-	15	-		-	30	4
<i>Tryb niestacjonarny</i>	9		-	15	-		-	24	
<i>Jednostka realizująca przedmiot, wydział:</i> Kolegium Nauk Społecznych									
<i>Odpowiedzialny za opracowanie karty przedmiotu (tytuł/stopień naukowy, imię i nazwisko, adres e-mail):</i> dr inż. Paweł Matuszczyk, pmatuszczyk@wszop.edu.pl									
CEL PRZEDMIOTU									
C1.	Poznanie przez studentów zasad bezpiecznego korzystania z systemów operacyjnych oraz metod zabezpieczania systemu, w tym zarządzania procesami systemowymi, aktualizacji systemu, wykonywania kopii zapasowych oraz								
C2.	Zapoznanie studentów z zasadami działania oraz możliwościami oprogramowania zabezpieczającego systemy operacyjne, w tym programów antywirusowych, programów do szyfrowania danych oraz stosowania haseł i ustawień								
C3.	Nabywanie przez studentów wiedzy z zakresu złośliwego oprogramowania i sposobów jego działania oraz metod zabezpieczania systemów przed takim oprogramowaniem..								
WYMAGANIA WSTĘPNE									
1.	Podstawowa wiedza z zakresu obsługi komputera oraz systemu operacyjnego Microsoft Windows.								
2.	Wiedza z zakresu Technologii Informacyjno-Komunikacyjnej na poziomie wyższych studiów inżynierskich.								

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ		METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ	ODNIESIENIE DO:	
			TREŚCI PROGRAMOWYCH	KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ
EU1	Student ma pogłębioną wiedzę z zakresu bezpieczeństwa systemów operacyjnych potrzebną do zabezpieczania komputera przed złośliwym oprogramowaniem oraz dostępem osób niepowołanych.	egzamin pisemny (pytania otwarte) sprawozdania z pracy indywidualnej	W1, W3, L2, L3	BWII K_W 04
EU2	Student potrafi skonfigurować system operacyjny w sposób minimalizujący ryzyko utraty danych oraz uszkodzenia systemu na skutek działania osób trzecich.	egzamin pisemny (pytania otwarte) sprawozdania z laboratorium	W2, W3, W4, L3, L4	BWII K_U 02
EU3	Student zna zasady działania złośliwego oprogramowania i jest świadomy zagrożeń, jakie może za sobą nieść.	demonstracja umiejętności praktycznych	W4, W5, L4, L	BWII K_U 06
TREŚCI PROGRAMOWE				
L.p.	WYKŁAD	Liczba godzin		
		S	N	
W1	Omówienie tematyki przedmiotu oraz zasad jego zaliczenia. Zasady bezpiecznego korzystania z systemów operacyjnych.	3	3	
W2	Podatność systemu operacyjnego na zagrożenia z zewnątrz. Metody ataków - złośliwe oprogramowanie, wirusy, spyware, backdoor.	3	3	
W3	Polecenie „Uruchom” oraz edytor rejestru systemowego.	3	3	
W4	Metody zabezpieczenia i konfiguracji systemu z wykorzystaniem wbudowanych narzędzi systemowych – stosowanie haseł, uprawnienia użytkowników, wykonywanie aktualizacji, zarządzanie procesami aktywnymi, tworzenie kopii zapasowej.	3	3	
W5	Metody zabezpieczenia systemu przed dostępem osób nieuprawnionych z wykorzystaniem dodatkowego oprogramowania - -antywirus, firewall, szyfrowanie danych.	3	3	
RAZEM		15	15	
FORMA I KRYTERIA ZALICZENIA WYKŁADU: egzamin pisemny (pytania otwarte) - ocena jakościowa,				
L.p.	LABORATORIUM	Liczba godzin		
		S	N	
L1	Konfiguracja systemu operacyjnego w celu osiągnięcia najwyższego poziomu bezpieczeństwa, przy wykorzystaniu wbudowanych narzędzi systemowych.	4	2	
L2	Wykorzystanie dodatkowego oprogramowania w celu zwiększenia poziomu bezpieczeństwa systemu operacyjnego. Konfiguracja stosowanego oprogramowania.	4	2	
L3	Weryfikacja stopnia zabezpieczenia systemu operacyjnego i skuteczności stosowanego oprogramowania przy wywołaniu ataków na system z innego komputera w sieci.	4	2	
L4	Zabezpieczenie danych na drodze szyfrowania z wykorzystaniem różnych metod i oprogramowania.	3	3	
RAZEM		15	9	
FORMA I KRYTERIA ZALICZENIA LABORATORIUM: demonstracja umiejętności praktycznych - ocena jakościowa, diagnostyczne studium przypadku -				
METODY I FORMY DYDAKTYCZNE				

1.	wykład informacyjny		
2.	wykład problemowy		
3.	ćwiczenia laboratoryjne		
NARZĘDZIA DYDAKTYCZNE			
1.	prezentacja multimedialna		
2.	interaktywne platformy do współpracy		
	biblioteki cyfrowe i zasoby online		
OPROGRAMOWANIE			
1.	MS Powerpoint		
2.	Zarządzanie komputerami ITManager		
	Vmware Workstation		
OBCIĄŻENIE STUDENTA PRACĄ			
Forma aktywności		Liczba godzin na zrealizowanie aktywności	
		<i>tryb stacjonarny</i>	<i>tryb niestacjonarny</i>
1.	godziny kontaktowe z nauczycielem akademickim	30	24
2.	samodzielne przygotowanie się do zajęć	17	23
3.	przygotowanie do zaliczenia/egzaminu	25	25
4.	Konsultacje	2	2
5.	zapoznanie się z literaturą	25	25
6.	zaliczenie/egzamin	1	1
SUMA GODZIN		100	100
LICZBA PUNKTÓW ECTS		4	4
LITERATURA PODSTAWOWA			
1.	Cole, E, <i>Bezpieczeństwo sieci</i> , Gliwice 2005		
2.	Szelaąg A., <i>Windows 10 PL. Optymalizacja i zaawansowane zarządzanie systemem.</i> , Gliwice 2015		
3.	Stallings, W., <i>Kryptografia i bezpieczeństwo sieci komputerowych</i> , Gliwice 2012		
LITERATURA UZUPEŁNIAJĄCA I ŹRÓDŁA PRAWA			
1.	Kosiński J., <i>Paradygmaty cyberprzestępczości</i> , Warszawa 2015		
2.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560)		
INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE:			
1.	PLATFORMA MOODLE zawiera: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ kierunkowe efekty uczenia się ▪ karty przedmiotów ▪ terminy konsultacji nauczycieli akademickich 		
4.	WIRTUALNY DZIEKANAT zawiera: <ul style="list-style-type: none"> ▪ harmonogram zajęć na bieżący semestr ▪ harmonogram sesji egzaminacyjnej ▪ ogłoszenia dotyczące organizacji roku akademickiego 		

5.	<p>Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny jakościowej oznacza, że zakładane efekty zostały osiągnięte:</p> <ul style="list-style-type: none"> ▪ 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.	<p>Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny ilościowej oznacza, że zakładane efekty zostały osiągnięte:</p> <ul style="list-style-type: none"> ▪ 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