Podhalańska Państwowa Uczelnia Zawodowa w Nowy Targu

Informacje ogólne

Nazwa zajęć	Bezpieczeństwo cybernetyczne
Kod zajęć	BN-1-5,4,21-22
Status zajęć	Obowiązkowy
Wydział / Instytut	Instytut Humanistyczno - Społeczny
Kierunek studiów	bezpieczeństwo narodowe
Moduł specjalizacyjny	-----
Specjalizacja	-----

Forma studiów	**Rok studiów**	**Semestr**	**Suma godzin dydaktycznych**		**Liczba punktów ECTS**
			Wykłady	**Ćwiczenia/praktyki**	
Stacjonarne	1	1	---	---	---
	1	2	---	---	---
	2	3	---	---	---
	2	4	---	---	---
	3	5	15.0	15.0	2.0
	Suma		**15.0**	**15.0**	**2.0**

Poziom studiów	studia pierwszego stopnia
Profil	Praktyczny
Osoba odpowiedzialna za program zajęć	dr Ryszard Lelito

Wymagania (Kompetencje wstępne)	Brak
Założenia i cele zajęć	Celem zajęć jest nabycie wiedzy przez studentów o zagrożeniach cybernetycznych (informatycznych) występujących w współczesnym świecie oraz sposobach im przeciwdziałania. Zajęcia powinny wykształtować u studentów umiejętności umysłowe (myślenie logiczne) w poznaniu zagrożeń cybernetycznych Uczestnictwo w zajęciach ma dać studentom zdolność wykorzystania nabytej wiedzy i umiejętności w pracy zawodowej lub dalszej nauce
Prowadzący zajęcia	mgr Robert Sito, dr Tomasz Wałek
Egzaminator/ Zaliczający	mgr Robert Sito, dr Tomasz Wałek

Nakład pracy studenta - bilans punktów ECTS

Nakład pracy studenta niezbędny do uzyskania efektów uczenia się	**Obciążenie studenta**			
	Studia stacjonarne		**Studia niestacjonarne**	
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów, w tym:	godz.: 35.0		godz.: 0.0	
Udział w wykładach (godz.)	15		0	
Udział w: ćwiczenia (godz.)	15		0	
Dodatkowe godziny kontaktowe z nauczycielem (godz.)	3		0	
Udział w egzaminie (godz.)	2		0	
Obciążenie studenta związane z jego indywidualną pracą związaną z zajęciami organizowanymi przez uczelnię, w tym:	godz.: 24.0		godz.: 0.0	
Samodzielne studiowanie tematyki zajęć/ przygotowanie się do wykładu (godz.)	5		0	
Samodzielne studiowanie tematyki zajęć/ przygotowanie się do: ćwiczenia (godz.)	5		0	
Przygotowanie do zaliczenia/ egzaminu (godz.)	4		0	
Wykonanie prac zaliczeniowych (referat, projekt, prezentacja itd.) (godz.)	10		0	
Suma (obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia oraz związane z jego indywidualną pracą związaną z tymi zajęciami)	godz.: 59.0	ECTS: 2.0	godz.: 0.0	ECTS: 0
Obciążenie studenta w ramach zajęć kształtujących umiejętności praktyczne	godz.: 0	ECTS: 0	godz.: 0	ECTS: 0

Efekty uczenia się

	Odniesienia

Efekty uczenia się		Odniesienia do kierunkowych efektów uczenia się	do charakterystyk drugiego stopnia efektów uczenia się Polskich Ram Kwalifikacji	Sposób weryfikacji efektów uczenia się
Wiedza: student zna i rozumie				
W1	zna przyczyny i następstwa wystąpienia zagrożeń systemów informatycznych, ma także wiedzę na temat pomiaru i oceny poziomu bezpieczeństwa tych systemów	K_W11	P6S_WG	odpowiedź, (W), udział w dyskusji, (W)
W2	zna rodzaje i klasyfikacje zagrożeń, a także modele i klasy bezpieczeństwa systemów informatycznych	K_W11	P6S_WG	
Umiejętności: student potrafi				
U1	potrafi wykryć wybrane zagrożenia w systemach informatycznych i wprowadzić określone zabezpieczenia	K_U11	P6S_UW_02	bezpośrednia ocena wykonania zadania (np. ocena projektu, ocena sprawozdania, dokumentowania danych, realizacji zajęć) (U)
Kompetencje społeczne: student jest gotów do				
K1	ma świadomość konieczności permanentnego doskonalenia i aktualizowania swojej wiedzy informatycznej.	K_K01	P6S_KK_01	ocena wypowiedzi (treści i sposobu jej przedstawiania;) (K)

Formy i metody kształcenia

dyskusja, praca w grupach, studium przypadku

Treści programowe

Wykłady

Pojęcie bezpieczeństwa systemu informatycznego, podatność zasobów i ryzyko wystąpienia zagrożeń, przyczyny i następstwa wystąpienia zagrożeń. Pomiar i ocena poziomu bezpieczeństwa systemów informatycznych.

Modele i klasy bezpieczeństwa systemów informatycznych (TCSEC, ITSEC, CCITSE).

Klasyfikacja zagrożeń SI, zagrożenia spowodowane przez działania ludzi, awarie urządzeń, programów i

infrastruktury, braki i uchybienia organizacyjne, zdarzenia losowe.

Prawne wymogi w zakresie bezpieczeństwa systemów informatycznych. Standardy oraz normy polskie i międzynarodowe w zakresie bezpieczeństwa SI (ISO, Polskie Normy, BSI, FIBS, RFC, CERT).

Zabezpieczenia systemu informatycznego i ich podział; zabezpieczenia fizyczne, zabezpieczenia techniczne: kopie zapasowe, ochrona przed wirusami, dobór i ochrona haseł, zabezpieczenia biometryczne, narzędzia kryptograficzne, steganografia, systemy firewall, systemy wykrywania włamań, zabezpieczenia organizacyjne, zabezpieczenia personalne, procedury ochronne i awaryjne.

Ćwiczenia

ćwiczenia

Zabezpieczenia systemu informatycznego i ich podział; zabezpieczenia fizyczne, zabezpieczenia techniczne: kopie zapasowe, ochrona przed wirusami, dobór i ochrona haseł, zabezpieczenia biometryczne, narzędzia kryptograficzne, steganografia, systemy firewall, systemy wykrywania włamań, zabezpieczenia organizacyjne, zabezpieczenia personalne, procedury ochronne i awaryjne.

Kryteria oceny osiągniętych efektów uczenia się

Kryteria oceny efektów uczenia się osiągniętych przez studenta	Na ocenę 5,0 Wyczerpujące odpowiedzi na 3 zadane pytania Na ocenę 4,5 Wystarczające choć niekompletne odpowiedzi. Dwie odpowiedzi powinny być kompletne. Na ocenę 4,0 wiedza podstawowa, wymagająca uzupełnienia. Przynajmniej jedna odpowiedź jest kompletna Na ocenę 3,5 wiedza elementarna w każdym zadanym obszarze Na ocenę 3,0 wiedza zawierająca znaczące braki, ale zaświadczająca o elementarnej wiedzy odpowiadającego. Student nie wykazuje wiedzy w jednym obszarze, ale posiada przynajmniej rozbudowaną wiedzę przy dwóch pozostałych zagadnieniach Na ocenę 2,0 student nie przystąpił do ustnego odpytania, lub nie wykazał się wiedzą świadczącą o

	chociażby elementarnej wiedzy

Forma weryfikacji osiągnięć studenta i warunki zaliczenia zajęć

Forma weryfikacji osiągnięć studenta	Zaliczenie z oceną
Warunki odbywania i zaliczenia zajęć oraz dopuszczenia do końcowego egzaminu (zaliczenia z oceną)	1. obecność na wykładach i ćwiczeniach 2. aktywność w czasie dyskusji na zaproponowane tematy 3. spełnienie wszystkich dodatkowych wymagań, które określi koordynator przedmiotu

Wykaz zalecanego piśmiennictwa

Wykaz literatury podstawowej

Lp.	Pozycja
1	F. Wołowski, J. Zawiła - Niedźwiedzki, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi. Kraków 2012
2	K. Liderman, Bezpieczeństwo informacyjne, Warszawa 2012
3	A. Szmonik, Organizacja i funkcjonowanie systemów bezpieczeństwa, Warszawa 2011

Wykaz literatury uzupełniającej

Lp.	Pozycja
1	A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Warszawa 2007
2	K. Liderman , Analiza ryzyka i ochrona informacji w systemach komputerowych. Warszawa 2009

Wymiar, zasady i forma odbywania praktyk zawodowych

Wymiar, zasady i forma odbywania praktyk zawodowych	-----

Wygenerowano: 2022-10-06 17:45:21.308170, BN-1-22-23