POLITECHNIKA BYDGOSKA
Wydział Zarządzania

Karta przedmiotu

Cyberbezpieczeństwo w systemie finansowym

1. Informacje podstawowe

Kierunek studiów finanse i rachunkowość **Specjalność** - **Jednostka zarządzająca kierunkiem studiów** Wydział Zarządzania **Poziom studiów** pierwszego stopnia (lic.) **Profil studiów** Profil praktyczny **Forma studiów** studia stacjonarne	**Cykl kształcenia (nabór)** 2023/24 **Kod przedmiotu** 08FIR-PS.PL8C.0317.23 **Języki wykładowe** polski **Obligatoryjność** Fakultatywny **Blok zajęciowy** Przedmioty kierunkowe

Wymagania wstępne	Swobodne poruszanie się po zasobach internetowych.
Przedmioty wprowadzające	Technologie informacyjne
Koordynator	Kinga Krupcała

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 4	• Wykład: 15, Zaliczenie na ocenę	2

2. Efekty uczenia się dla przedmiotu

Kod	**Opis efektów uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**	**Odniesienie do charakterystyk PRK**

Kod	Opis efektów uczenia się	Odniesienie do kierunkowych efektów uczenia się	Odniesienie do charakterystyk PRK
Wiedza:			
W1	Zna elementarną terminologię dotyczącą cyberbezpieczeństwa. Zna ryzyko w cyberprzestrzeni i rodzaje zabezpieczeń.	FIR_P1_K_W02, FIR_P1_K_W06, FIR_P1_K_W13	P6S_WG, P6S_WK, P6S_WK, P6S_WK
Umiejętności:			
U1	Potrafi rozróżnić techniki włamań i metody ochrony przed nimi. Prowadzi działania mające ustrzec przez najczęściej popełnianymi błędami w ochronie zasobów informacyjnych (w tym głównie finansowych).	FIR_P1_K_U01, FIR_P1_K_U03, FIR_P1_K_U09	P6S_UW, P6S_UW, P6S_UK
Kompetencje społeczne:			
K1	Jest otwarty na nowe podejścia do bezpieczeństwa w Sieci. Rozróżnia i identyfikuje zagrożenia informatyczne, szczególnie z zakresu finansów i rachunkowości.	FIR_P1_K_K01, FIR_P1_K_K03	P6S_KK, P6S_KK

3. Treści programowe

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
1.	1. Bezpieczeństwo informacyjne, cyberprzestrzeń i jej rodzaje, cyberatak, konflikt asymetryczny. 2. Cyberbezpieczeństwo, zasady ochrony zasobów informatycznych, normy dotyczące bezpieczeństwa zasobów, rodzaje zagrożeń bezpieczeństwa informacyjnego. 3. Błędy w ochronie zasobów, techniki włamań do systemów, system zarządzania bezpieczeństwem organizacji. 4. Zarządzanie ryzykiem, metody ograniczania ryzyka zagrożenia. 5. Certyfikaty cyfrowe, podpis elektroniczny.	Wykład	W1, U1, K1

4. Metody prowadzenia zajęć, weryfikacji efektów uczenia się i warunki zaliczenia

Forma zajęć	

Wykład	**Metody prowadzenia zajęć:**	
	Wykład	
	Metody (sposoby) weryfikacji:	**Udział:**
	Zaliczenie pisemne	100%
	Warunki zaliczenia przedmiotu:	
	Warunkiem zaliczenia przedmiotu jest zaliczenie na min. 60% (8,5 pkt) testu pisemnego dotyczącego wszystkich treści prezentowanych podczas wykładów i składającego się z 8 pytań zamkniętych (każde pytanie 1 pkt) oraz 8 pytań otwartych (każde pytanie 1 pkt, ale jest możliwość otrzymania również 0,5 pkt za połowicznie poprawną odpowiedź). Osoby, które otrzymały ocenę pozytywną z zaliczenia w pierwszym terminie i były aktywne (aktywnie uczestniczyły w dyskusji podczas wykładów - min. 3 plusy) - będą miały podniesioną ocenę z zaliczenia pisemnego o pół stopnia w górę (nie dotyczy to osób, które nie zaliczyły testu w pierszym terminie lub z testu otrzymały ocenę bardzo dobry). Obecność na wszystkich wykładach jest obowiązkowa.	

Efekt uczenia się dla przedmiotu	**Metody (sposoby) weryfikacji**
	Zaliczenie pisemne
W1	x
U1	x
K1	x

5. Literatura

Literatura podstawowa

1. Szczepankiewicz E., 2018, Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach - wyniki badań [w:] „Zeszyty Teoretyczne Rachunkowości" tom 97 (153), 2018, s. 115−138.
2. Wrzosek M., 2013, Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego, Wydawnictwo Menedżerskie PTM
3. Bączek P., 2006, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek
4. Januszewski A., 2011, Funkcjonalność informatycznych systemów zarządzania. Tom 1 Zintegrowane systemy transakcyjne, Wyd. Nauk. PWN
5. Liderman K., 2012, Bezpieczeństwo informacyjne, Wyd. Nauk. PWN

Literatura uzupełniająca

1. Oleński J., 2003, Ekonomika informacji. Metody, Wyd. PWE
2. Zaskórski P., Szwarc K., 2013, Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania, [w:] Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki Nr 9, Rok 7, 2013, s. 37-52.
3. Swanson M., Bowen P., Wohl Phillips A., Gallup D., Lynes D., 2010, Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34, May 2010, http://csrc. nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
4. Flakiewicz W., 2002, Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje, Wyd. C.H. Beck
5. Liderman K., 2009, Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego, „Biuletyn Instytutu Automatyki i Robotyki", nr 26, Wyd. WAT

6. Nakład pracy studenta - bilans godzin i punktów ECTS

Aktywność studenta		Obciążenie studenta Liczba godzin
Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia	Wykład	15
Praca własna studenta	Konsultacje	10
	Przygotowanie do zajęć	10
	Studiowanie literatury	10
	Przygotowanie do zaliczenia	15
Łączny nakład pracy studenta		60
Liczba punktów ECTS		2

* Godzina (dydaktyczna) oznacza 45 minut