KARTA KURSU

Nazwa	POLITYKA BEZPIECZEŃSTWA INFORMACJI NIEJAWNYCH
Nazwa w j. ang.	SECURITY INFORMATION POLICY

Kod		Punktacja ECTS*	1

Koordynator	dr Jarosław Jastrzębski	Zespół dydaktyczny

Opis kursu (cele kształcenia)

W toku realizacji przedmiotu student ma zapoznać się ze strukturą sporządzania dokumentacji polityki bezpieczeństwa informacji niejawnych w organizacjach. Poprzez udział w zajęciach i samodzielne studiowanie literatury studenci mają wiedzieć na czym polega realizacja polityki bezpieczeństwa na po szczególnych poziomach organizacyjnych i zarządzania zarówno w organizacjach nastawionych na zysk, jak i w jednostkach administracji publicznej.

Warunki wstępne

Wiedza	Student zna podstawowe pojęcia oraz instytucje prawne z zakresu ochrony informacji niejawnych.
Umiejętności	Student potrafi pracować nad tekstami normatywnymi.
Kursy	Nie wymagane

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01 Student posiada poszerzoną wiedzę dotyczącą rozwiązań prawno – organizacyjnych, form i metod ochrony informacji niejawnych. W02 Student zna w sposób dogłębny zasady rządzące ochroną informacji niejawnych mających wpływ na bezpieczeństwo wewnętrzne państwa.	Sp2bi_W02 Sp2bi_W03

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01 Student potrafi wykorzystać zdobytą wiedzę do prawidłowej oceny zjawisk zachodzących w obszarze bezpieczeństwa informacyjnego państwa. U02 Student potrafi sporządzić krytyczną ocenę zjawisk zachodzących w obszarze bezpieczeństwa informacyjnego państwa.	Sp2bi_U01 Sp2bi_U03

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01 Student prawidłowo rozwiązuje problemy, dotyczące działalności sektora państwowego i prywatnego w zakresie ochrony informacji niejawnych. K02 Student posiada świadomość dotyczącą profesjonalizmu i etycznego kontekstu podejmowanych działań z zakresu ochrony informacji niejawnych.	Sp2bi_K01 Sp2bi_K03

Organizacja												
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin	15	-		-		-		-		-		-

Opis metod prowadzenia zajęć

Wykład monograficzny połączony z dyskusją na kluczowe problemy omawiane w trakcie kursu.

Formy sprawdzania efektów kształcenia

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01	-	-	-	-	-	-	-	Tak	-	-	-	-	-
W02	-	-	-	-	-	-	-	Tak	-	-	-	-	-
U01	-	-	-	-	-	-	-	Tak	-	-	-	-	-
U02	-	-	-	-	-	-	-	Tak	-	-	-	-	-
K01	-	-	-	-	-	-	-	Tak	-	-	-	-	-
K02	-	-	-	-	-	-	-	Tak	-	-	-	-	-

Kryteria oceny	Uzyskanie zaliczenia wymaga: - obecności i aktywności podczas zajęć - uczestnictwa w dyskusjach

Uwagi	-

Treści merytoryczne (wykaz tematów)

1. Strategia bezpieczeństwa organizacji - cele globalne
2. Ogólna polityka bezpieczeństwa
3. Polityka bezpieczeństwa fizycznego
4. Polityka bezpieczeństwa systemów teleinformatycznych
5. Zadania poszczególnych pionów strukturalnych organizacji w zakresie realizacji polityki bezpieczeństwa
6. Dokumenty i ich struktura oraz zasady opracowania.

Wykaz literatury podstawowej

Ochrona informacji niejawnych, Warszawa 2007.
Ustawa z dnia 5 sierpnia 2010 o ochronie informacji niejawnych, (Dz.U. 2010.187.1228)
Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948)
Rozporządzenia Ministra Obrony Narodowej z dnia 2. listopada 2011 r., w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji nie jawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, rozdział VI i VII.
Technika informatyczna- wytyczne do zarządzania systemów informatycznych. Pojęcie i modele bezpieczeństwa systemów informatycznych, PN-I- 13 bezpieczeństwa systemów informatycznych, Część 2 : Zarządzanie i planowanie bezpieczeństwa systemów informatycznych, ISO/ICE TR 13335-2. Warszawa 2003.

Technika informatyczna – wytyczne do zarządzania bezpieczeństwem systemów informatycznych, Część 3: Techniki zarządzania bezpieczeństwem systemów informatycznych, ISO/IEC TR 13335-3, Warszawa 2003.

Wykaz literatury uzupełniającej

T. Szewc, Ochrona informacji niejawnych, Warszawa 2007.
A. Żebrowski, Wywiad i kontrwywiad w XXI wieku, Lublin 2011.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Ilość godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	-
	Pozostałe godziny kontaktu studenta z prowadzącym	-
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	-
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	-
	Przygotowanie do egzaminu	-
Ogółem bilans czasu pracy		30
Ilość punktów ECTS w zależności od przyjętego przelicznika		1