KARTA KURSU

Nazwa	Zarządzanie ryzykiem w bezpieczeństwie informacyjnym
Nazwa w j. ang.	Risk management in information security

Koordynator	**dr Piotr Swoboda**	Zespół dydaktyczny: dr Piotr Swoboda

Punktacja ECTS*	**1**

Opis kursu (cele kształcenia)

Celem kształcenia jest zapoznanie uczestników kursu z podstawowymi aspektami zarządzania bezpieczeństwem informacji w zakresie rozwiązań systemowych, jak również na poziomie jednostki organizacyjnej, w szczególności z uwzględnieniem podejścia opartego na ryzyku (na przykładzie ochrony danych osobowych).

Warunki wstępne

Wiedza	Student posiada podstawową wiedzę z zakresu nauk społecznych.
Umiejętności	Student potrafi zidentyfikować podstawowe problemy bezpieczeństwa z punktu widzenia państwa, jak również konkretnej jednostki organizacyjnej oraz potrafi tworzyć logiczne powiązania między różnymi zjawiskami i procesami.
Kursy	Administracja, bezpieczeństwo państwa, bezpieczeństwo wewnętrzne, politologia.

Efekty uczenia się:

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01, Student dysponuje wiedzą na temat najważniejszych pojęć, zagrożeń i problemów z zakresu bezpieczeństwa informacji.	W03 BI_W01, BI_W03
	W02, Student posiada wiedzę na temat organizacji systemu bezpieczeństwa informacji.	W03, W04, W06, W07 BI_W01, BI_W02
	W03, Student zna podstawowe metody i narzędzia oceny i szacowania ryzyka bezpieczeństwa informacji oraz postępowania z ryzkiem w zarządzaniu organizacją.	W02, W03, W05, W06 BI_W02, BI_W03 BI_W04

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01, Student potrafi zidentyfikować najważniejsze zagrożenia dla bezpieczeństwa informacji oraz ich konsekwencje dla państwa i jednostek organizacyjnych oraz użytkowników systemów przetwarzających.	U01, U02, U04 BI_U01
	U02, Student jest w stanie zidentyfikować podstawowe procesy związane z zarządzaniem ryzykiem w organizacji.	U01, U02, U03, U05 BI _U01
	U03, Student potrafi dokonywać prostych czynności w zakresie oceny i szacowania ryzyka dla bezpieczeństwa informacji.	U01, U03, U04, U05, U06 BI_U01, BI _U03

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01, Student ma świadomość ryzyka dla bezpieczeństwa informacji przetwarzanych przez podmioty prywatne i publiczne, w szczególności w odniesieniu do zagrożeń występujących w cyberprzestrzeni.	K01, K02 BI_K01
	K02, Student rozumie złożoność otoczenia wewnętrznego i zewnętrznego współczesnych organizacji w szczególności w kontekście bezpieczeństwa zasobów informacyjnych.	K01 BI_K01
	K03, Student jest świadomy ról uczestników procesu zarządzania bezpieczeństwem informacji na różnych poziomach zarządzania organizacją.	K03 BI_K02, BI_K03

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

Opis metod prowadzenia zajęć

Wykłady: – Prezentacja Power Point; – Dyskusja na podstawie studium przypadku; – Symulacja.

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	x					x		x					
W02	x					x		x					
W03	x					x		x					
U01	x					x		x					
U02	x					x		x					
U03	x					x		x					
K01	x					x		x					
K02	x					x		x					
K03	x					x		x					

Kryteria oceny	Obecność na wykładach. Realizacja projektu indywidualnego (symulacja szacowania i oceny ryzyka).

Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącym zajęcia po przedstawieniu zgody na indywidualny tok studiów. Przepisanie oceny z kursu o tej samej nazwie (lub zbliżonej) realizowanego na tym samym stopniu kształcenia warunkowane jest ekwiwalentną liczbą godzin, punktów ECTS oraz co najmniej oceną dobrą. Odrobienie nieobecności na zajęciach – wykonanie dodatkowej pracy po indywidualnym ustaleniu z prowadzącym.

Treści merytoryczne (wykaz tematów)

1) Uwagi wstępne na temat organizacji procesu zarządzania ryzykiem bezpieczeństwa informacji w organizacji.
2) Podstawy prawne oraz wybrane normy, wytyczne, standardy, zalecenia oraz podejścia dotyczące zarządzania ryzykiem w bezpieczeństwie informacji.
3) Podstawowe pojęcia dotyczące zarządzania ryzykiem oraz sposoby rozumienia podejścia opartego na ryzyku w ochronie danych osobowych.
4) Etapy szacowania ryzyka.
5) Wybrane przykłady sposobów i metod szacowania ryzyka na różnych etapach i poziomach zarządzania ryzykiem w bezpieczeństwie informacji i danych osobowych – ogólna ocena ryzyka (analiza ryzyka), ocena skutków dla ochrony danych (DPIA), ocena ryzyka w zarządzaniu incydentami bezpieczeństwa; Propozycje optymalnych rozwiązań.

Wykaz literatury podstawowej

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) dnia 27 kwietnia 2016 r., Dz.Urz.UE.L nr 119, str. 1 z późn. zm.;

2) *Jak rozumieć podejście oparte na ryzyku?, Poradnik RODO. Podejście oparte na ryzyku*. Część 1, GIODO 2017;
3) *Jak stosować podejście oparte na ryzyku?, Poradnik RODO. Podejście oparte na ryzyku*. Część 2, GIODO 2017;
4) Generalny Inspektor Ochrony Danych Osobowych, *Wskazówki i narzędzia pomocne w dokonywaniu oceny skutków dla ochrony danych*, https://archiwum.giodo.gov.pl/pl/1520281/10482.

Wykaz literatury uzupełniającej

1) Anzel M., *Ocena ryzyka oraz ocena skutków dla ochrony przetwarzanych danych osobowych*. Przykład metody szacowania ryzyka opartej na gotowych macierzach, One1;
2) Daniluk P., *Bezpieczeństwo i zarządzanie. Analiza strategiczna*, Warszawa 2015;
3) E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002;
4) Łuczak J., Trybulski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/ IEC 27001*, Poznań 2009;
5) Wróblewski (red.), *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, CNBOP-PIB, Józefów 2015;
6) Pełnomocnik Rządu ds. Cyberbezpieczeństwa, *Zarządzanie ryzykiem bezpieczeństwa informacji Przegląd struktury organizacyjnej, misji i systemu informatycznego*, Warszawa 2022;
7) *Recommendations for a methodology of the assessment of severity of personal data breaches*, ENISA 2013;
8) Normy ISO (PN-ISO/IEC 27001, 27002, 27005, 27018).

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	-
	Pozostałe godziny kontaktu studenta z prowadzącym	-
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna)	5
	Przygotowanie do egzaminu/zaliczenia	-
Ogółem bilans czasu pracy		25
Liczba punktów ECTS w zależności od przyjętego przelicznika		1