KARTA KURSU

Nazwa	Zarządzanie ryzykiem cyberbezpieczeństwa
Nazwa w j. ang.	Cyber security risk management

Kod		Punktacja ECTS*	3

Koordynator	dr Piotr Swoboda	Zespół dydaktyczny
		dr Piotr Swoboda

Opis kursu (cele kształcenia)

Celem kształcenia jest zapoznanie uczestników kursu z podstawowymi aspektami zarządzania ryzykiem bezpieczeństwa informacji i cyberbezpieczeństwa w zakresie rozwiązań systemowych, jak również na poziomie jednostki organizacyjnej, w szczególności z uwzględnieniem wybranych metod szacowania i oceny ryzyka.

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	Bezpieczeństwo państwa, bezpieczeństwo wewnętrzne, cyberbezpieczeństwo, administracja.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01, Student dysponuje wiedzą na temat najważniejszych pojęć, zagrożeń i problemów z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa. W02, Student posiada wiedzę na temat organizacji systemu zarządzania cyberbezpieczeństwem oraz bezpieczeństwa informacji. W03, Student zna podstawowe metody i narzędzia oceny i szacowania ryzyka bezpieczeństwa informacji oraz postępowania z ryzykiem w zarządzaniu organizacją.	K_W07, KW_08, KW_09.

	Efekt kształcenia 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. U02, Student jest w stanie zidentyfikować podstawowe procesy związane z zarządzaniem ryzykiem w organizacji. U03, Student potrafi dokonywać prostych czynności w zakresie oceny i szacowania ryzyka dla bezpieczeństwa informacji, w szczególności odnoszących się do cyberprzestrzenii.	K_U05, K_U09, K_U010, K_U011.

	Efekt kształcenia 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. K02, Student rozumie złożoność otoczenia wewnętrznego i zewnętrznego współczesnych organizacji w szczególności w kontekście bezpieczeństwa zasobów informacyjnych. K03, Student jest świadomy ról uczestników procesu zarządzania ryzykiem cyberbezpieczeństwa i bezpieczeństwem informacji na różnych poziomach zarządzania organizacją.	K_K01, K_K04, K_K05.

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	E				
Liczba godzin	10	15									

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A	K	L	S	P	E				
Liczba godzin	5	10									

Opis metod prowadzenia zajęć

Wykłady i ćwiczenia: – 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	x					
W02	x		x				x	x					
W03	x		x				x	x					
U01	x		x				x	x					
U02	x		x				x	x					
U03	x		x				x	x					
K01	x		x				x	x					
K02	x		x				x	x					
K03	x		x				x	x					

Kryteria oceny	Obecność i aktywność na zajęciach. Realizacja projektu grupowego (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) Podstawowe pojęcia dotyczące zarządzania ryzykiem cyberbezpieczeństwa oraz sposoby rozumienia podejścia opartego na ryzyku w bezpieczeństwie organizacji. 2) Podstawy prawne oraz wybrane normy, wytyczne, standardy, zalecenia oraz podejścia dotyczące zarządzania ryzykiem i bezpieczeństwa informacji. 3) Uwagi wstępne na temat organizacji procesu zarządzania ryzykiem w organizacji. 4) Struktura procesu zarządzania ryzykiem. Poziomy i etapy zarządzania ryzykiem. 5) Wybrane przykłady sposobów i metod szacowania ryzyka na różnych etapach i poziomach zarządzania ryzykiem w bezpieczeństwie informacji na przykładzie systemu ochrony 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) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t. j. Dz. U. 2023, poz. 913 (z późn. zm.).
2) Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwer, Warszawa 2023 (wyd. 2).
3) Marzec E., *Pojęcie ryzyka w regulacji cyberbezpieczeństwa*, „Monitor Prawniczy" 2020 nr 23.
4) *Jak rozumieć podejście oparte na ryzyku?,* Poradnik RODO. Podejście oparte na ryzyku. Część 1, GIODO 2017.
5) *Jak stosować podejście oparte na ryzyku?,* Poradnik RODO. Podejście oparte na ryzyku. Część 2, GIODO 2017.
6) Generalny Inspektor Ochrony Danych Osobowych, *Wskazówki i narzędzia pomocne w dokonywaniu oceny skutków dla ochrony danych*, https://archiwum.giodo.gov.pl/pl/1520281/10482.
7) Polski Komitet Normalizacyjny, *Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania*, PN-EN ISO/IEC 27001:2017-06P.

Wykaz literatury uzupełniającej

1) Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, t. j. Dz. U. 2017, poz. 209 (z późn. zm.).
2) Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t. j. Dz. U. 2022, poz. 1648 (z późn. zm.).
3) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz.U. 2023 poz. 756 (z późn. zm.).
4) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz.U. 2011 nr 159 poz. 948.
5) 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.).
6) Rozporządzenie Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. 2017, poz. 2247).
7) Wróblewski D. (red.), *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, CNBOP-PIB, Józefów 2015.
8) Daniluk P., *Bezpieczeństwo i zarządzanie. Analiza strategiczna*, Difin, Warszawa 2015.
9) Anzel M., *Ocena ryzyka oraz ocena skutków dla ochrony przetwarzanych danych osobowych. Przykład metody szacowania ryzyka opartej na gotowych macierzach*, One1.
10) Denning E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
11) Łuczak J., Trybulski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009.
12) Fundacja Bezpieczeństwa Informacji Polska, *Metodyka zarządzania ryzykiem w ochronie danych osobowych*, Warszawa 2018, http://fbipolska.pl/FBI_Metodyka_10.pdf.
13) NASK – PINB, *ABC cyberbezpieczeństwa*, Warszawa 2022.
14) Polski Komitet Normalizacyjny, *Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji*, PN-EN ISO/IEC 27002:2017-06P.
15) Polski Komitet Normalizacyjny, *Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji*, PN-ISO/IEC 27005:2014-01P.
16) *Recommendations for a methodology of the assessment of severity of personal data breaches*, ENISA 2013.
17) Pełnomocnik Rządu ds. Cyberbezpieczeństwa, *Zarządzanie ryzykiem bezpieczeństwa informacji Przegląd struktury organizacyjnej, misji i systemu informatycznego*, Warszawa 2022.
18) Agencja Wywiadu, Ministerstwo Cyfryzacji, *Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych RP oraz innych państw NATO w kontekście wybranych ataków hakerskich,* 2023: https://www.gov.pl/web/baza-wiedzy/analiza-zagrozen-dla-cyberbezpieczenstwa-placowek-dyplomatycznych-nato.

19) Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* Warszawa 2015.
20) *Strategia Cyberbezpieczeństwa RP na lata 2019 – 2024,* Ministerstwo Cyfryzacji, Warszawa 2019.
21) *Największe zagrożenia dla bezpieczeństwa w Internecie w 2016 roku. Głos polskich ekspertów,* Raport, Fundacja Bezpieczna Cyberprzestrzeń, 2016.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) - **studia stacjonarne**

Ilość godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	25
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	-
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	30
	Przygotowanie do egzaminu	
Ogółem bilans czasu pracy		75
Ilość punktów ECTS w zależności od przyjętego przelicznika		3

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) - **studia niestacjonarne**

Ilość godzin w kontakcie z prowadzącymi	Wykład	5
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	25
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	-
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	30
	Przygotowanie do egzaminu	
Ogółem bilans czasu pracy		75
Ilość punktów ECTS w zależności od przyjętego przelicznika		3