KARTA KURSU

Nazwa	Bezpieczeństwo informacji niejawnych i danych osobowych
Nazwa w j. ang.	Security of Classified Information and Personal Data

Koordynator	dr Piotr Swoboda	Zespół dydaktyczny
		dr Piotr Swoboda dr Paulina Motylińska
Punktacja ECTS*	3	

Opis kursu (cele kształcenia)

Celem kształcenia jest zapoznanie uczestników kursu z podstawowymi pojęciami i problemami z zakresu bezpieczeństwa informacji, a także dostarczenie podstawowej wiedzy na temat podstaw prawnych, zasad przetwarzania oraz organizacji i funkcjonowania systemów bezpieczeństwa oraz ochrony informacji niejawnych i danych osobowych.

Warunki wstępne

Wiedza	Student posiada podstawową wiedzę z zakresu nauk społecznych.
Umiejętności	Student potrafi zidentyfikować podstawowe elementy systemu bezpieczeństwa państwa.
Kursy	Administracja, bezpieczeństwo państwa, bezpieczeństwo wewnętrzne, bezpieczeństwo międzynarodowe, politologia, stosunki międzynarodowe.

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.	W02, W03
	W02, Student posiada pogłębioną wiedzę na temat podstaw prawnych, organizacji i funkcjonowania systemu ochrony informacji niejawnych oraz systemu ochrony danych osobowych.	W02, W04, W06
	W03, Student zna role i obowiązki podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa informacji niejawnych oraz danych osobowych w systemie bezpieczeństwa państwa oraz na poziomie jednostek organizacyjnych.	W02, W04, W06,

	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. U02, Student potrafi dokonywać interpretacji przepisów prawa oraz zasad ochrony informacji niejawnych i danych osobowych. U03, Student samodzielnie identyfikuje powiązania instytucjonalne w systemach bezpieczeństwa informacji niejawnych oraz danych osobowych i potrafi odpowiednio wskazać podmioty odpowiedzialne za przeciwdziałanie określonym rodzajom zagrożeń dla bezpieczeństwa informacji.	U01, U02, U04 U03 U02, U04

	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. K02, Student zna funkcjonowanie systemów ochrony informacji niejawnych i danych osobowych oraz rozumie kompetencje poszczególnych podmiotów odpowiedzialnych w tym zakresie na poziomie jednostek organizacyjnych. K03, Student jest świadomy w zakresie wymogów prawnych, jak również możliwości korzystania ze stosownych procedur oraz wykorzystania odpowiednich narzędzi w zakresie zgłaszania nieprawidłowości i wprowadzania optymalnych rozwiązań w przedmiocie organizacji systemów ochrony informacji niejawnych oraz danych osobowych na poziomie jednostek organizacyjnych.	K1_K02 K1_K01, K1_K03 K1_K03

Organizacja												
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin	20	10										E

Opis metod prowadzenia zajęć

Wykłady: – prezentacja Power Point; Ćwiczenia: - Zajęcia prowadzone są w grupie audytoryjnej. Studenci wykonują ćwiczenia samodzielne i/lub grupowe na każdych zajęciach oraz przedstawiają efekty swojej pracy na forum grupy.

Formy sprawdzania efektów uczenia się

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

Kryteria oceny	Obecność na wykładach i ćwiczeniach. Egzamin pisemny z problematyki poruszanej na wykładach, znajomości podstawowych aktów prawnych oraz literatury obowiązkowej przedmiotu, wskazanych przez prowadzącego.

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.

Treści merytoryczne (wykaz tematów)

Wykład:

I. Wprowadzenie.

1) Ochrona informacji niejawnych a ochrona danych osobowych i inne tajemnice prawnie chronione.
2) Podstawowe atrybuty bezpieczeństwa informacji.
3) Zagrożenia bezpieczeństwa informacji.

II. Bezpieczeństwo danych osobowych.

1) Przesłanki filozoficzne i historia ochrony danych osobowych.
2) Podstawy prawne ochrony danych osobowych.
3) System ochrony danych osobowych w Polsce i UE.
4) Podstawowe pojęcia.
5) Zasady ochrony danych osobowych.

6) Organizacja i zarządzanie bezpieczeństwem i ochroną danych osobowych.

III. Bezpieczeństwo informacji niejawnych.

1) Historia ochrony informacji niejawnych w Polsce.
2) Podstawy prawne ochrony informacji niejawnych.
3) Podstawowe pojęcia.
4) Klasyfikacja informacji niejawnych w Polsce i w NATO.
5) System ochrony informacji niejawnych w Polsce.
6) Organizacja i zarządzanie bezpieczeństwem i ochroną informacji niejawnych.

Ćwiczenia:

1) Ogólne rozporządzenie o ochronie danych – analiza zawartości dokumentu.
2) Naruszenia bezpieczeństwa informacji – analiza przypadków (m.in. typ naruszenia, przyczyny, skutki, podjęte działania).
3) Zagrożenia bezpieczeństwa informacji – rodzaje, typologie, skutki.
4) Klauzule informacyjne – analiza zawartości.
5) Bezpieczeństwo informacji niejawnych – nadawanie klauzuli tajności, poświadczenie bezpieczeństwa, postępowania sprawdzające (ankieta bezpieczeństwa osobowego).
6) Naruszenia ochrony informacji niejawnych – analiza wyroków sądowych.
7) Bezpieczeństwo danych osobowych – szacowanie i ocena ryzyka.

Wykaz literatury podstawowej

Bezpieczeństwo i ochrona danych osobowych:

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) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, t.j. Dz.U. 2019 poz. 1781.
3) Banyś T. A. J., Kuba M., Łuczak J., Bielak-Jomaa E., *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, Difin, Warszawa 2016.
4) Swoboda P., *Bezpieczeństwo danych osobowych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1, red. O. Wasiuta, R. Klepka, AT Wydawnictwo, Wydawnictwo LIBRON- Filip Lohner, Kraków 2019.
5) Swoboda P., Bezpieczeństwo danych osobowych, [w:] Encyklopedia bezpieczeństwa, t. 1, A – C, red. O. Wasiuta, S. Wasiuta, Wydawnictwo LIBRON - Filip Lohner, Kraków 2021.

Bezpieczeństwo i ochrona informacji niejawnych:

1) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz.U. 2024 poz. 632 z późn. zm.
2) Zalewski S., *Informacje niejawne we współczesnym świecie*, Editions Spotkania, 2018.
3) Swoboda P., *Bezpieczeństwo informacji niejawnych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1, red. O. Wasiuta, R. Klepka, AT Wydawnictwo, Wydawnictwo LIBRON - Filip Lohner, Kraków 2019.
4) Swoboda P., Bezpieczeństwo informacji niejawnych, [w:] Encyklopedia bezpieczeństwa, t. 1, A – C, red. O. Wasiuta, S. Wasiuta, Wydawnictwo LIBRON - Filip Lohner, Kraków 2021.

Wykaz literatury uzupełniającej

Bezpieczeństwo i ochrona danych osobowych:

1) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.
2) Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz.U. 2023 poz. 1206.
3) Litwiński P., *Książeczka o danych osobowych*, Barta-Litwiński, Kraków 2024, https://www.bartalitwinski.pl/Ksiazeczka%20o%20danych%20osobowych.epub.
4) Jabłoński M., Jarosz-Żukowska S., *Prawa człowieka i systemy ich ochrony. Zarys wykładu*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2004.
5) Agencja Praw Podstawowych UE, Rady Europy, Kancelaria Europejskiego Trybunału Praw Człowieka, *Podręcznik europejskiego prawa o ochronie danych*, Urząd Publikacji UE, Luksemburg 2014, www.giodo.gov.pl/pl/file/6755.
6) Kępa L., *Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców*, C.H. Beck, Warszawa 2018.
7) NASK-Państwowy Instytut Badawczy, ABC Cyberbezpieczeństwa, Warszawa 2022, https://it-szkola.edu.pl/publikacje,plik,90.
8) Sakowska-Baryła M., Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, C.H. Beck, Warszawa 2018.
9) Śmiałek K., Kominek A. (red.), *Ochrona danych osobowych. Perspektywa krajowa i międzynarodowa*, Wydawnictwo Naukowe FNCE, 2021.
10) Sobczyk A., RODO. Rozproszona władza publiczna, WUJ, Kraków 2019.
11) UODO, MEN, Ochrona danych osobowych w szkołach i placówkach oświatowych. Poradnik RODO, sierpień 2018.
12) Zalecenia, wytyczne i poradniki Prezesa Urzędu Ochrony Danych Osobowych:
    Jak rozumieć podejście oparte na ryzyku?, Poradnik RODO. Podejście oparte na ryzyku. Część 1, GIODO 2017.
    Jak stosować podejście oparte na ryzyku?, Poradnik RODO. Podejście oparte na ryzyku. Część 2, GIODO 2017.
13) Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, UODO 2018.
14) Strona internetowa UODO: www.uodo.gov.pl.

Bezpieczeństwo i ochrona informacji niejawnych:

1) Barcz J., Libera B., *Urzędnik i biznesmen w środowisku międzynarodowym*, Wolters Kluwer Polska, Warszawa 2007.
2) Jakubus B., Ryszkowski M., *Ochrona informacji niejawnych*, Wydawnictwo Projekt, Warszawa 2001.
3) Hoc S., Szewc T., Ochrona danych osobowych i informacji niejawnych, C.H. Beck, Warszawa 2014.
4) Zalewski S., *Dylematy ochrony informacji niejawnych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2009.
5) Wociór D. (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, C.H. Beck, Warszawa 2016.
6) Gajos M. (red.), *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych/Uniwersytet Śląski w Katowicach, Katowice 2011.
7) Goryński G., *Prawne podstawy ochrony informacji niejawnych w Polsce*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych" 2013 nr 1, s. 99-128.
8) Swoboda P., *Wywiad i kontrwywiad w Polsce w procesie przemian systemowych (1989 – 2007)*, Wydawnictwo Avalon, Kraków 2016.

9) Swoboda P., *Funkcjonowanie systemu dostępu do informacji publicznej w Polsce w kontekście współczesnych zagrożeń dla bezpieczeństwa państwa, [w:] Informacyjny wymiar bezpieczeństwa państw i jednostek*, red. W. Fehler, Uniwersytet Przyrodniczo Humanistyczny w Siedlcach, Siedlce 2021.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

liczba godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	-
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna)	10
	Przygotowanie do egzaminu/zaliczenia	15
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3