

UCHWAŁA NR 415 /XXIV/XV/2019
Senatu Politechniki Białostockiej
z dnia 18 kwietnia 2019 roku

- w sprawie ustalenia programu studiów podyplomowych Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych

Senat Politechniki Białostockiej, działając na podstawie art. 28 ust. 1 pkt 11 i 15 lit. a ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668, z późn. zm.), postanawia:

§ 1

Ustalić program studiów podyplomowych Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych, stanowiący załącznik do niniejszej uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

REKTOR

prof. dr hab. inż. Lech Dzieńis



Załącznik do Uchwały Nr 415/XXIV/XV/2018 Senatu PB



WYDZIAŁ INŻYNIERII ZARZĄDZANIA
POLITECHNIKI BIAŁOSTOCKIEJ

PROGRAM STUDIÓW PODYPLOMOWYCH

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – INSPEKTOR OCHRONY DANYCH

P.O. KIEROWNIK
SEKCJI JAKOŚCI KSZTAŁCENIA
Politechniki Białostockiej

J. Kręowska
dr inż. Joanna Kręowska

Białystok, 2019 r.

PROREKTOR
do. Kształcenia i Współpracy Międzynarodowej

L. Kowalik
dr hab. inż. Katarzyna Kowalik, prof. zw.

DZIEKAN
WYDZIAŁU INŻYNIERII ZARZĄDZANIA
Politechniki Białostockiej

J. Ejdys
dr hab. inż. Joanna Ejdys, prof. zw.

**PROGRAM STUDIÓW PODYPLOMOWYCH
ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – INSPEKTOR OCHRONY DANYCH**

Studia podyplomowe Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych trwają 2 semestry i umożliwiają uzyskanie kwalifikacji cząstkowych na poziomie 6 PRK. Łączna liczba punktów ECTS: 30. Łączna liczba godzin zajęć: 170.

**Plan studiów
ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – INSPEKTOR OCHRONY DANYCH**

zatwierdzony Uchwałą Rady Wydziału Inżynierii Zarządzania z dnia 6 lutego 2019 r.

	Nazwa przedmiotu	Godziny			Punkty ECTS	Forma zaliczenia
		w.	ćw.	razem		
SEMESTR I						
1.	Współczesne problemy zarządzania	3	3	6	1	ZO
2.	Zarządzanie bezpieczeństwem informacji w sektorze publicznym i prywatnym	6	6	12	3	ZO
3.	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony danych osobowych	8	8	16	3	E
4.	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony informacji niejawnych	8	8	16	3	E
5.	Organizacja i funkcjonowanie kancelarii tajnych	4	4	8	1	ZO
6.	Inspektor Ochrony Danych – rola, obowiązki, odpowiedzialność	4	4	8	2	ZO
7.	Praktyczne aspekty wdrażania RODO	8	8	16	3	ZO
SEMESTR II						
1.	Normy bezpieczeństwa i ochrona informacji w organizacji	8	8	16	3	ZO
2.	Budowa i funkcjonowanie systemu ochrony danych osobowych	4	4	8	1	ZO
3.	Informatyka śledcza z elementami hackingu – metody i środki ochrony danych	8	8	16	3	ZO
4.	Ochrona danych osobowych w przedsiębiorstwie i administracji publicznej – studia przypadków	8	8	16	3	ZO
5.	Etyka zawodowa w zarządzaniu informacją	4	4	8	1	ZO
6.	Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017	12	12	24	3	E
Razem semestr I		41	41	82	16	
Razem semestr II		44	44	88	14	
RAZEM		85	85	170	30	

ZO – zaliczenie na ocenę, E - egzamin

SYLWETKA ABSOLWENTA

Program studiów dostosowany jest do wymagań współczesności oraz kształtujących ją norm i trendów związanych z bezpieczeństwem informacji.

Absolwent Studiów Podyplomowych Zarządzanie Bezpieczeństwem Informacji - Inspektor Ochrony Danych posiada:

- wiedzę, umiejętności i kompetencje w zakresie ochrony danych osobowych niezbędną do wykonywania funkcji Inspektora Ochrony Danych (IOD);
- niezbędne przygotowanie do pracy na stanowiskach związanych z ochroną informacji niejawnych i udostępnianiem informacji publicznej;
- umiejętności z zakresu ochrony i bezpieczeństwa przetwarzania danych osobowych w działalności instytucji publicznych i sektora prywatnego;
- wiedzę w zakresie funkcjonowania systemu ochrony danych osobowych i informacji niejawnych na gruncie prawa międzynarodowego i polskiego;
- umiejętności w zakresie stosowania metod i środków ochrony informacji.

Absolwenci studiów uzyskują kwalifikacje pozwalające zajmować stanowiska pracy jako Inspektorzy Ochrony Danych (IOD) oraz wiedzę z zakresu zarządzania bezpieczeństwem informacji.

Wiedza i umiejętności będą miały charakter zarządczy, prawny i technologiczny. Dodatkowo, podczas zajęć dydaktycznych poruszane będą aspekty społeczne i etyczne zarządzania bezpieczeństwem informacji.

Absolwenci Studiów Podyplomowych Zarządzanie Bezpieczeństwem Informacji - Inspektor Ochrony Danych uzyskują dodatkowe kwalifikacje audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017 potwierdzone certyfikatem.

OPIS KOMPETENCJI OCZEKIWANYCH OD KANDYDATA UBIEGAJACEGO SIĘ O PRZYJĘCIE NA STUDIA PODYPLOMOWE

Uczestnikiem studiów podyplomowych może być osoba, która posiada kwalifikację pełną co najmniej na poziomie 6 PRK uzyskaną w systemie szkolnictwa wyższego i nauki.

ZESTAWIENIE TABELARYCZNE KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ ODNOŚĄCYCH SIĘ DO CHARAKTERYSTYK DRUGIEGO STOPNIA OKREŚLONYCH NA PODSTAWIE USTAWY Z DNIA 22 GRUDNIA 2015 R. O ZINTEGROWANYM SYSTEMIE KWALIFIKACJI NA POZIOMIE 6 PRK

Załącznik nr 1 do „Wytyczne do tworzenia programów studiów podyplomowych”

Symbol	Efekty uczenia się dla studiów podyplomowych	Odniesienie do charakterystyk drugiego stopnia określonych na podstawie art. 7 ust. 3 Ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji na poziomie 6 PRK	Odniesienie do charakterystyk drugiego stopnia określonych na podstawie art. 7 ust. 4 Ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji na poziomie 6 PRK
Wiedza: absolwent zna i rozumie			
ZBI_W1	istotę oraz cele nowoczesnego zarządzania, w szczególności zarządzania bezpieczeństwem informacji w organizacji	P6S_WG	P6Z_WT, P6Z_WZ, P6Z_WO
ZBI_W2	zagrożenia oraz skutki wynikające z niewłaściwego przechowywania i przetwarzania danych	P6S_WG, P6S_WK	P6Z_WZ
ZBI_W3	zasady funkcjonowania systemów zarządzania bezpieczeństwem i ochroną danych osobowych na gruncie prawa międzynarodowego i polskiego	P6S_WG, P6S_WK	P6Z_WT, P6Z_WZ, P6Z_WO
ZBI_W4	zasady funkcjonowania systemów zarządzania bezpieczeństwem i ochroną informacji niejawnych na gruncie prawa międzynarodowego i polskiego	P6S_WG, P6S_WK	P6Z_WT, P6Z_WZ, P6Z_WO
ZBI_W5	obszary i cele audytu informatycznego oraz metody i narzędzia wykorzystywane w informatyce śledczej	P6S_WG, P6S_WK	P6Z_WO
ZBI_W6	najważniejsze teorie etyczne w kontekście bezpieczeństwa informacji	P6S_WK	P6Z_WT
Umiejętności: absolwent potrafi			
ZBI_U1	wykorzystać wiedzę z zakresu koncepcji, metod i technik zarządzania w różnych sytuacjach oraz adoptować je do specyficznych warunków zarządzania bezpieczeństwem informacji w organizacji	P6S_UW	P6Z_UI, P6Z_UO
ZBI_U2	zidentyfikować obszary i procesy biznesowe w organizacji, w których dochodzi do przetwarzania informacji, w szczególności danych osobowych	P6S_UW	P6Z_UI, P6Z_UO
ZBI_U3	zarządzać bezpieczeństwem informacji w organizacji	P6S_UW P6S_UO	P6Z_UI, P6Z_UO
ZBI_U4	przeprowadzić analizę ryzyka i zagrożeń bezpieczeństwa informacji w organizacji oraz dobierać środki adekwatne do zidentyfikowanych ryzyk	P6S_UW	P6Z_UI, P6Z_UO
ZBI_U5	wskazać i wykorzystać właściwe narzędzia informatyczne wspomagające wdrażanie systemu ochrony danych osobowych	P6S_UW	P6Z_UI, P6Z_UO, P6Z_UN

ZBI_U6	wykorzystać zdobytą wiedzę do analizy i rozstrzygnięcia etycznego problemu	P6S_UW	P6Z_UI, P6Z_UO
ZBI_U7	przewodzić audyty wewnętrzne systemu zarządzania bezpieczeństwem informacji	P6S_UW, P6S_UO	P6Z_UI, P6Z_UO
ZBI_U8	komunikować się i współdziałać w grupie na potrzeby zarządzania bezpieczeństwem informacji w organizacji	P6S_UO, P6S_UK	P6Z_UI, P6Z_UO
ZBI_U9	planować własny rozwój zawodowy i podległych mu pracowników w zakresie pełnionej funkcji Inspektora Ochrony Danych	P6S_UU	P6Z_UU
Kompetencje społeczne: absolwent jest gotów do			
ZBI_K1	współpracy i kształtowania właściwych relacji zawodowych w organizacji	P6S_KO	P6Z_KP, P6Z_KW
ZBI_K2	krytycznego oceniania posiadanej wiedzy	P6S_KK	P6Z_KP
ZBI_K3	odpowiedzialnego pełnienia roli Inspektora Ochrony Danych oraz przestrzegania zasad etyki	P6S_KR, P6S_KO	P6Z_KP, P6Z_KO

MATRYCA EFEKTÓW UCZENIA SIĘ

Załącznik nr 2 do „Wytoczne do tworzenia programów studiów poddyplomowych”

Nazwa studiów poddyplomowych: Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych																										
MATRYCA POKRYCIA EFEKTÓW UCZENIA SIĘ																										
Lp.	nazwa przedmiotu	kod przedmiotu	semestr	WIEDZA							UMIEJĘTNOŚCI															
				ZBL_W1	ZBL_W2	ZBL_W3	ZBL_W4	ZBL_W5	ZBL_W6	kod przedmiotu	ZBL_U1	ZBL_U2	ZBL_U3	ZBL_U4	ZBL_U5	ZBL_U6	ZBL_U7	ZBL_U8	ZBL_U9	ZBL_K1	ZBL_K2	ZBL_K3	kod przedmiotu			
1.	Współczesne problemy zarządzania	SPZBI01	I	X														X							SPZBI01	
2.	Zarządzanie bezpieczeństwem informacji w sektorze publicznym i prywatnym	SPZBI02	I		X													X								SPZBI02
3.	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony danych osobowych	SPZBI03	I			X												X								SPZBI03
4.	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony informacji niejawnych	SPZBI04	I				X											X								SPZBI04
5.	Organizacja i funkcjonowanie kancelarii tajnych	SPZBI05	I				X											X								SPZBI05
6.	Inspektor Ochrony Danych – rola, obowiązki, odpowiedzialność	SPZBI06	I			X												X								SPZBI06
7.	Praktyczne aspekty wdrażania RODO	SPZBI07	I	X		X												X	X							SPZBI07
1.	Normy bezpieczeństwa i ochrona informacji w organizacji	SPZBI08	II			X													X							SPZBI08
2.	Budowa i funkcjonowanie systemu ochrony danych osobowych	SPZBI09	II			X													X							SPZBI09
3.	Infomatyka śledcza z elementami hackingu – metody i środki ochrony danych	SPZBI10	II					X											X							SPZBI10
4.	Ochrona danych osobowych w przedsiębiorstwie i administracji publicznej – studia przypadków	SPZBI11	II			X													X							SPZBI11
5.	Etyka zawodowa w zarządzaniu informacją	SPZBI12	II																X							SPZBI12
6.	Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017	SPZBI13	II			X																X				SPZBI13
suma:				2	1	7	2	1	1	1	2	5	8	3	1	1	1	1	3	2	2	1	1	2	3	

RAMOWE PROGRAMY PRZEDMIOTÓW

Karty przedmiotów zgodne ze wzorem - Załącznik nr 1 do Zarządzenia Nr 915 z 2019 r. Rektora PB

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Współczesne problemy zarządzania							Kod przedmiotu	SPZBI01
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	3	3						Punkty ECTS	1
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest dostarczenie wiedzy z tego zakresu oraz praktycznych umiejętności ich wykorzystania w procesie zarządzania informacją.								
Treści programowe	Wykład: istota i cele nowoczesnego zarządzania. Paradoxy zarządzania. Wyzwania w zarządzaniu potencjałem ludzkim organizacji. Koncepcje zarządzania. Ćwiczenia: metody i techniki zarządzania. Zarządzanie a zmiany w makro i mikrootoczeniu organizacji.								
Metody dydaktyczne	wykład problemowy, burza mózgów, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz wskazuje istotę oraz cele nowoczesnego zarządzania. Prawidłowo identyfikuje paradoxy zarządzania.							ZBI_W1	
EU2	Słuchacz charakteryzuje zadania kadry kierowniczej w zarządzaniu potencjałem ludzkim organizacji i wskazuje sposoby ich efektywnej realizacji.							ZBI_W1	
EU3	Słuchacz dobiera metody i techniki zarządzania do różnych sytuacji, w tym kryzysowych oraz adoptuje nowoczesne koncepcje do specyficznych warunków swojego funkcjonowania w różnych stadiach wzrostu przedsiębiorstw.							ZBI_U1	
EU4	Słuchacz stosuje zasady właściwego zarządzania potencjałem ludzkim i umiejętnie utrzymuje relacje							ZBI_U1, ZBI_K1	

	w trakcie współpracy w środowisku zawodowym organizacji.	
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja
EU1	zaliczenie ustne	W
EU2	zaliczenie ustne	W
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.
Wyliczenie	udział w wykładach	3
	udział w ćwiczeniach	3
	udział w konsultacjach	1
	samodzielne studia literatury przedmiotu	12
	przygotowanie do zaliczenia ustnego z wykładu	6
	RAZEM:	25
Wskaźniki ilościowe		GODZINY ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		7 0,3
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		16 0,6
Literatura podstawowa	1. Moczydłowska J.M., Kowalewski K., Nowe koncepcje zarządzania ludźmi, Difin 2014. 2. Moczydłowska J.M., Paradoxy w zarządzaniu kapitałem ludzkim w ocenie menedżerów, „Nauki o Zarządzaniu” 2016, nr 2 (27), s. 130-138.	
Literatura uzupełniająca	1. Kuc B.R., Moczydłowska J.M., Zachowania organizacyjne, Difin 2009. 2. Moczydłowska J.M., Serafin K., Doskonalenie kompetencji zawodowych w profesjonalnie zarządzanej organizacji, Wydawnictwo Naukowe Sophia, Katowice 2016.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	dr hab. Joanna Moczydłowska, prof. PB	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Zarządzanie bezpieczeństwem informacji w sektorze publicznym i prywatnym							Kod przedmiotu	SPZBI02
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	6	6						Punkty ECTS	3
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest charakterystyka właściwości danych informatycznych ze szczególnym uwzględnieniem sposobów zachowania ich integralności, poufności oraz dostępności.								
Treści programowe	Wykład: informacja jako istotne aktywo w organizacji. Charakterystyka przetwarzania danych cyfrowych. Typowe działania i zaniechania powodujące naruszenie atrybutów danych informatycznych oraz ich skutki. Ćwiczenia: praktyczne aspekty przetwarzania danych cyfrowych. Metody zapewniające bezpieczeństwo informacji stanowiących tajemnicę przedsiębiorstwa. Narzędzia umożliwiające ochronę danych osobowych i innych danych o szczególnym znaczeniu w przedsiębiorstwie. Szkody majątkowe oraz pozamajątkowe wynikające z naruszenia bezpieczeństwa informacji.								
Metody dydaktyczne	wykład problemowy, studia przypadków, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz identyfikuje i analizuje obszary, w których informacja pełni istotną rolę w organizacji.							ZBI_U2	
EU2	Słuchacz opisuje i identyfikuje zagrożenia wynikające z niewłaściwego przechowywania i przetwarzania danych.							ZBI_W2, ZBI_U3	
EU3	Słuchacz stosuje mechanizmy zabezpieczające informacje.							ZBI_U3	
EU4	Słuchacz charakteryzuje działania i zaniechania nieprzestrzegania zasad bezpieczeństwa informacji skutkujących szkodami majątkowymi oraz pozamajątkowymi.							ZBI_W2	

Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja	
EU1	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
EU2	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C	
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
EU4	zaliczenie ustne	W	
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.	
Wyliczenie	udział w wykładach	6	
	udział w ćwiczeniach	6	
	udział w konsultacjach	1	
	wykonanie indywidualnych zadań ćwiczeniowych	15	
	samodzielne studia literatury przedmiotu	27	
	przygotowanie do zaliczenia ustnego z wykładu	20	
	RAZEM:	75	
Wskaźniki ilościowe		GODZINY	ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		13	0,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		49	2,0
Literatura podstawowa	<p>1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 1000).</p> <p>2. 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).</p> <p>3. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017.</p> <p>4. Kaczmarek T.T., Zarządzanie ryzykiem: ujęcie interdyscyplinarne, Difin, Warszawa 2010.</p>		
Literatura uzupełniająca	<p>1. Gałach A., Zarządzanie Bezpieczeństwem Informacji w Sektorze Publicznym, Wydawnictw C.H. Beck, Warszawa 2009.</p> <p>2. Jatkiewicz P., Uwarunkowania zarządzania systemem bezpieczeństwa informacji w jednostkach samorządu terytorialnego, Uniwersytet Gdański Wydział Zarządzania, Gdańsk 2012.</p>		
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu	
Program opracował(a)	mgr Dariusz Gromadka	15.01.2019	

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony danych osobowych							Kod przedmiotu	SPZBI03
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	8	8						Punkty ECTS	3
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z regulacjami prawnymi obejmującymi problematykę ochrony danych osobowych.								
Treści programowe	<p>Wykład: podstawy prawne ochrony danych osobowych. Określenie istoty zarządzania bezpieczeństwem danych osobowych w Polsce. Omówienie aktów prawnych regulujących ochronę danych osobowych w Polsce. System ochrony danych osobowych w Polsce. Zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych. Odpowiedzialność karna za naruszenie przepisów o ochronie danych osobowych. Międzynarodowe prawodawstwo w zakresie ochrony danych osobowych.</p> <p>Ćwiczenia: praktyczny aspekt ochrony danych osobowych w organizacjach. Zasady w systemie ochrony danych osobowych w Polsce. Elementy składowe systemu ochrony danych osobowych. Procedury postępowania w przypadku naruszenia przepisów o ochronie danych osobowych. Analiza studiów przypadku związanych z naruszeniami przepisów o ochronie danych osobowych. Analiza studiów przypadku dotyczących konsekwencji karnych wynikających z naruszenia przepisów o ochronie danych osobowych.</p>								
Metody dydaktyczne	wykład problemowy, studia przypadków, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład - egzamin pisemny; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz charakteryzuje podstawowe pojęcia związane z ochroną danych osobowych w Polsce.							ZBI_W3	
EU2	Słuchacz wskazuje, omawia i stosuje w praktyce akty							ZBI_W3, ZBI_U3	

	prawne dotyczące ochrony danych osobowych.	
EU3	Słuchacz wymienia i scharakteryzuje poszczególne elementy systemu ochrony danych osobowych w Polsce.	ZBI_W3
EU4	Słuchacz prawidłowo zachowuje się w przypadku zetknięcia z danymi osobowymi oraz stosuje procedury w przypadku naruszenia przepisów o ochronie danych osobowych.	ZBI_U2, ZBI_U3
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja
EU1	egzamin pisemny	W
EU2	egzamin pisemny (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C
EU3	egzamin pisemny	W
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.
Wyliczenie	udział w wykładach	8
	udział w ćwiczeniach	8
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	18
	samodzielne studia literatury przedmiotu	20
	przygotowanie do egzaminu pisemnego z wykładu	20
	RAZEM:	75
Wskaźniki ilościowe		GODZINY ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		17 0,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		47 1,9
Literatura podstawowa	1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000). 2. 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). 3. Gałaj-Emiliańczyk K., Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku, Difin S.A., Warszawa 2016. 4. Gawroński M., Ochrona danych osobowych: przewodnik po ustawie i RODO z wzorami, Wolters Kluwer, Warszawa 2018.	
Literatura uzupełniająca	1. Lubasz D., RODO: zmiany w zakresie ochrony danych osobowych: porównanie przepisów, praktyczne uwagi, Wolters Kluwer, Warszawa 2018. 2. Bandyś T.A.J. i in., Prawo ochrony danych osobowych: podręcznik dla studentów i praktyków. Difin, Warszawa, 2016.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	mgr Konrad Gałaj-Emiliańczyk	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony informacji niejawnych							Kod przedmiotu	SPZBI04
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	8	8						Punkty ECTS	3
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z regulacjami prawnymi obejmującymi problematykę ochrony informacji niejawnych.								
Treści programowe	Wykład: podstawy prawne ochrony informacji niejawnych. Pojęcie informacji niejawnych i jej znaczenie w organizacji. Omówienie definicji: bezpieczeństwa, bezpieczeństwa informacji i zarządzania bezpieczeństwem informacji. Zagadnienia wprowadzające: omówienie podstawowych aktów prawnych regulujących ochronę informacji prawnie chronionych w Polsce. Określenie istoty zarządzania bezpieczeństwem informacyjnym w Polsce. Istota informacji niejawnych w systemie demokratycznym państwa. Zasady w systemie ochrony informacji niejawnych w Polsce. Zakres podmiotowy i przedmiotowy ustawy o ochronie informacji niejawnych. Międzynarodowa wymiana informacji niejawnych. Ćwiczenia: praktyczny aspekt ochrony informacji prawnie chronionych w organizacjach. System ochrony informacji niejawnych w Polsce: klasyfikowanie informacji niejawnych, organizacja ochrony informacji niejawnych, bezpieczeństwo osobowe, bezpieczeństwo fizyczne, bezpieczeństwo teleinformatyczne, bezpieczeństwo przemysłowe. Elementy składowe systemu ochrony informacji niejawnych oraz organizacji ochrony informacji niejawnych w jednostce organizacyjnej. Procedury postępowania w przypadku naruszenia przepisów o ochronie informacji niejawnych. Odpowiedzialność karna za naruszenie przepisów o ochronie informacji niejawnych.								
Metody dydaktyczne	wykład problemowy, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – egzamin pisemny; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych	

		efektów uczenia się	
EU1	Sluchacz charakteryzuje podstawowe pojęcia związane z ochroną informacji niejawnych w Polsce.	ZBI_W4	
EU2	Sluchacz wskazuje, omawia i stosuje w praktyce akty prawne dotyczące ochrony informacji niejawnych.	ZBI_W4, ZBI_U2	
EU3	Sluchacz wymienia i charakteryzuje poszczególne elementy systemu ochrony informacji niejawnych w Polsce.	ZBI_W4	
EU4	Sluchacz prawidłowo zachowuje się w przypadku zetknięcia z informacją prawnie chronioną oraz stosuje procedury w przypadku naruszenia przepisów o ochronie informacji niejawnych.	ZBI_U2, ZBI_U3	
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja	
EU1	egzamin pisemny	W	
EU2	egzamin pisemny (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C	
EU3	egzamin pisemny	W	
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.	
Wyliczenie	udział w wykładach	8	
	udział w ćwiczeniach	8	
	udział w konsultacjach	1	
	wykonanie indywidualnych zadań ćwiczeniowych	15	
	samodzielne studia literatury przedmiotu	23	
	przygotowanie do egzaminu pisemnego z wykładu	20	
	RAZEM:	75	
Wskaźniki ilościowe		GODZINY	ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		17	0,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		47	1,9
Literatura podstawowa	1. Konstytucja RP z dnia 2 kwietnia 1997 r. 2. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, Nr 182, poz. 1228 z późn. zm.). 3. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. 1997, nr 88, poz. 553 z późn. zm.). 4. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. 2018, poz. 2096). 5. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).		
Literatura uzupełniająca	1. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001, nr 1497, poz. 229 z późn.zm.). 2. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 1993, nr 47, poz. 211 z późn. zm.).Rozporządzenie Rady Ministrów z dnia 7		

	<p>grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011, nr 276, poz.1631).</p> <p>3. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011, nr 288, poz. 1692).</p> <p>4. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948).</p>	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	podinsp. dr Agata Lasota-Jądrzak	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Organizacja i funkcjonowanie kancelarii tajnych							Kod przedmiotu	SPZBI05
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	4	4						Punkty ECTS	1
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest zapoznanie z wymogami prawa ochrony informacji niejawnych w związku z tworzeniem i funkcjonowaniem kancelarii tajnych.								
Treści programowe	Wykład: środki ochrony fizycznej informacji niejawnych (lokalizacja, wyposażenie i stosowanie środków ochrony fizycznej w kancelarii tajnej). Zasady organizacji i funkcjonowania kancelarii tajnych. Ćwiczenia: przyjmowanie, przewożenie, wydawanie i ochrona dokumentów niejawnych. Klasyfikacja informacji niejawnych. Zasady prowadzenia kancelaryjnych rejestrów ewidencyjnych. Weryfikacja dokumentów niejawnych. Podstawy archiwizacji.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz charakteryzuje zakres organizacji i funkcjonowania kancelarii tajnych.							ZBI_W4	
EU2	Słuchacz wskazuje i charakteryzuje wymagania przepisów prawa ochrony informacji niejawnych.							ZBI_W4	
EU3	Słuchacz wskazuje i wdraża zasady organizacji i funkcjonowania kancelarii tajnych. Posiada umiejętność weryfikowania systemu ochrony informacji niejawnych.							ZBI_W4, ZBI_U2	
EU4	Słuchacz poprawnie komunikuje się w zakresie zagadnień dotyczących problematyki ochrony informacji niejawnych i współdziała w grupie na potrzeby tworzenia							ZBI_U8	

	i organizacji kancelarii tajnych.		
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja	
EU1	zaliczenie ustne	W	
EU2	zaliczenie ustne	W	
EU3	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C	
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.	
Wyliczenie	udział w wykładach	4	
	udział w ćwiczeniach	4	
	udział w konsultacjach	1	
	wykonanie indywidualnych zadań ćwiczeniowych	9	
	przygotowanie do zaliczenia ustnego z wykładu	7	
	RAZEM:	25	
Wskaźniki ilościowe		GODZINY	ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		9	0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		14	0,6
Literatura podstawowa	<ol style="list-style-type: none"> 1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, Nr 182, poz. 1228 z późn. zm.). 2. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011, nr 276, poz. 1631). 3. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011, nr 288, poz. 1692). 4. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948). 5. Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. 2011, nr 93, poz. 541). 		
Literatura uzupełniająca	<ol style="list-style-type: none"> 1. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. 2011, nr 156, poz. 926). 2. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa, w sprawie wzoru decyzji o odmowie poświadczenia bezpieczeństwa osobowego (Dz.U. 2010, nr 258, poz. 1752). 3. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań 		

	<p>bezpieczeństwa przemysłowego (Dz.U. 2017, poz. 2334).</p> <p>4. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. 2012, poz. 683).</p> <p>5. Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. 2011, nr 93, poz. 541).</p>	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	podinsp. dr Agata Lasota-Jądrzak	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Inspektor Ochrony Danych – rola, obowiązki, odpowiedzialność							Kod przedmiotu	SPZBI06
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	4	4						Punkty ECTS	2
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest przedstawienie roli oraz obowiązków Inspektora Ochrony Danych w organizacji.								
Treści programowe	<p>Wykład: zawód Inspektor Ochrony Danych - perspektywy pracy, zarobki, zapotrzebowanie. Wymagania i kwalifikacje Inspektora Ochrony Danych. Rola Inspektora Ochrony Danych w organizacji. Zakres obowiązków Inspektora Ochrony Danych. Inspektor w strukturze organizacji kontra zewnętrzny doradca – możliwości, zakres odpowiedzialności. Dodatkowe kompetencje Inspektora Ochrony Danych.</p> <p>Ćwiczenia: problemy pojawiające się w pracy Inspektora Ochrony Danych. Analiza zagrożeń bezpieczeństwa informacji w organizacji. Bezpieczeństwo, ciągłość oraz integralność danych. Perspektywy dla zawodu wynikające z przepisów unijnych oraz postępu technologicznego.</p>								
Metody dydaktyczne	wykład problemowy, studia przypadku, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz wymienia i omawia obowiązki, kompetencje i kwalifikacje Inspektora Ochrony Danych wynikające z krajowych i unijnych przepisów o ochronie danych osobowych.							ZBI_W3	
EU2	Słuchacz przeprowadza analizę zagrożeń bezpieczeństwa informacji w organizacji.							ZBI_U4	
EU3	Słuchacz wymienia i charakteryzuje zasady oraz planuje i							ZBI_W3, ZBI_U3	

	prowadzi nadzór nad bezpieczeństwem, ciągłością oraz integralnością danych.	
EU4	Śluchacz krytycznie oceniając posiadaną wiedzę planuje dalsze kierunki rozwoju zawodowego własnego i podległych pracowników w pełnieniu funkcji Inspektora Ochrony Danych.	ZBI_K2, ZBI_U9
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja
EU1	zaliczenie ustne	W
EU2	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU3	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.
Wyliczenie	udział w wykładach	4
	udział w ćwiczeniach	4
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	11
	samodzielne studia literatury przedmiotu	20
	przygotowanie do zaliczenia ustnego z wykładu	10
	RAZEM:	50
Wskaźniki ilościowe		GODZINY ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		9 0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		36 1,4
Literatura podstawowa	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) 2. Domagała M. i in., Nowe standardy w ochronie danych osobowych, Wydawnictwo Think & Make, Warszawa 2018. 3. Bielak-Jomaa E., Lubasz D. (red.), Polska i europejska reforma ochrony danych osobowych, Wolters Kluwer, Warszawa 2016.	
Literatura uzupełniająca	1. Galaj-Emiliańczyk K., Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów (z suplementem elektronicznym), Wydawnictwo dla Biznesu ODDK, Warszawa 2018. 2. Czub-Kielczewska S., ABC ochrony danych osobowych w bibliotece, Medialex 2016.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	mgr Sylwia Czub-Kielczewska	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Praktyczne aspekty wdrażania RODO							Kod przedmiotu	SPZBI07
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	1
	8	8						Punkty ECTS	3
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest zapoznanie z poszczególnymi etapami wdrożenia przepisów ogólnego rozporządzenia o ochronie danych (RODO) w organizacji.								
Treści programowe	Wykład: etapy wdrożenia przepisów ogólnego rozporządzenia o ochronie danych (RODO) w organizacji. Obowiązek informacyjny. Ćwiczenia: wyznaczenie zespołu wdrożeniowego. Harmonogram wdrożenia. Identyfikacja procesów przetwarzania danych osobowych. Inwentaryzacja zasobów. Budowanie rejestru czynności. Ocena skutków przetwarzania danych (DPIA – Data Protection Impact Assessment). Szacowanie ryzyka w zasobach. Przykłady wdrożeń w przedsiębiorstwach.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz wymienia i charakteryzuje etapy wdrażania systemu ochrony danych osobowych w organizacji.							ZBI_W3	
EU2	Słuchacz organizuje zespół wdrożeniowy oraz przygotowuje harmonogram wdrożenia systemu ochrony danych osobowych w organizacji.							ZBI_U3	
EU3	Słuchacz definiuje i opisuje procesy biznesowe funkcjonujące w organizacji, podczas których dochodzi do przetwarzania danych osobowych oraz dokonuje inwentaryzacji zasobów.							ZBI_W1, ZBI_U2	
EU4	Słuchacz opracowuje treść obowiązku informacyjnego dla							ZBI_U3	

	zidentyfikowanego procesu oraz rejestr czynności przetwarzania prowadzony przez administratora danych.	
EU5	Sluchacz ocenia skutki przetwarzania danych i analizuje ryzyka w zasobach.	ZBI_U4
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja
EU1	zaliczenie ustne	W
EU2	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU3	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU5	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.
Wyliczenie	udział w wykładach	8
	udział w ćwiczeniach	8
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	12
	samodzielne studia literatury przedmiotu	29
	przygotowanie do zaliczenia ustnego z wykładu	17
	RAZEM:	75
Wskaźniki ilościowe		GODZINY ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		17 0,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		50 2
Literatura podstawowa	1. Banyś T., Łuczak J., Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, PRESSCOM, Wrocław 2017. 2. Gawroński M., Ochrona danych osobowych: przewodnik po ustawie i RODO z wzorami, Wolters Kluwer, Warszawa 2018. 3. Lubasz D., RODO: zmiany w zakresie ochrony danych osobowych: porównanie przepisów, praktyczne uwagi, Wolters Kluwer, Warszawa 2018. 4. Gałaj-Emiliańczyk K., Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku, Difin S.A., Warszawa 2016.	
Literatura uzupełniająca	1. Strona internetowa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl 2. Krasuski A., Ochrona danych osobowych na podstawie RODO, wyd. Wolters Kluwer Polska, Warszawa 2018. 3. Bargiel-Kaflik M. i in., Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, C.H. Beck, Warszawa 2017.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	mgr Marta Rejner, mgr Sylwia Czub-Kielczewska	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Normy bezpieczeństwa i ochrona informacji w organizacji							Kod przedmiotu	SPZBI08
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	2
	8	8						Punkty ECTS	3
Przedmioty wprowadzające	Zarządzanie bezpieczeństwem informacji w sektorze publicznym i prywatnym								
Cele przedmiotu	Celem przedmiotu jest zapoznanie z wymogami sformalizowanego podejścia do ochrony informacji w organizacji i ryzyk związanych z jej przetwarzaniem na bazie norm związanych z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) – PN-ISO/IEC 27001:2017-06 oraz oceną ryzyka informacji PN-ISO/IEC 27005:2014-01.								
Treści programowe	Wykład: informacja jawna i chroniona oraz jej zasoby. Umocowanie ustawowe grup informacji będących aktywem i zasobem organizacji/ przedsiębiorstwa/ korporacji w systemie prawa polskiego i międzynarodowego. SZBI w organizacji – jego bliższe i dalsze otoczenie systemowe. Rodzina norm bezpieczeństwa ISO 27k i jej znaczenie dla ochrony informacji. Ćwiczenia: analiza zagrożeń bezpieczeństwa informacji w organizacji. Ocena ryzyka dla aktywów informacyjnych organizacji. Wykorzystanie norm ISO 31000, ISO 31010 i ISO 27005 w analizie ryzyk. Przykłady analizy ryzyka w organizacji.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz charakteryzuje wymagania znormalizowanych systemów zarządzania bezpieczeństwem i ochroną informacji (SZBI/ISMS).							ZBI_W3	
EU2	Słuchacz charakteryzuje wymagania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz jego Deklaracji Stosowania zgodnie z normą PN-ISO/IEC 27001:2017-06.							ZBI_W3	
EU3	Słuchacz wdraża wybrane elementy SZBI w dowolnej jednostce organizacyjnej, waliduje jego							ZBI_U3	

	stosowanie w ramach zintegrowanego systemu zarządzania jakością i bezpieczeństwem w firmie.	
EU4	Słuchacz komunikuje się w zakresie zagadnień dotyczących problematyki bezpieczeństwa i ochrony informacji, omawia zakres komunikacji wewnętrznej i zewnętrznej w ramach SZBI oraz współdziała w grupie na potrzeby analizy zagrożeń i oceny ryzyk informacyjnych oraz wdrażania systemu.	ZBI_W3, ZBI_U8
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja
EU1	zaliczenie ustne	W
EU2	zaliczenie ustne	W
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU4	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.
Wyliczenie	udział w wykładach	8
	udział w ćwiczeniach	8
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	15
	samodzielne studia literatury przedmiotu	23
	przygotowanie do zaliczenia ustnego z wykładu	20
	RAZEM:	75
Wskaźniki ilościowe		GODZINY ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		17 0,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		47 1,9
Literatura podstawowa	1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017. 2. Sitaniec I., Zawila-Niedźwiecki J. (red.), Ryzyko operacyjne w naukach o zarządzaniu, C.H. Beck, Warszawa 2015. 3. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa -Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018.	
Literatura uzupełniająca	1. PN-ISO/IEC 27002:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji, wyd. PKN, Warszawa 2018. 2. PN-ISO/IEC 27005:2014-01, Technika informatyczna – Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014. 3. Polaczek T. Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice 2006.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	dr inż. Marek Blim, dr inż. Dariusz Kłosowski	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Budowa i funkcjonowanie systemu ochrony danych osobowych							Kod przedmiotu	SPZBI09
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	2
	4	4						Punkty ECTS	1
Przedmioty wprowadzające	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony danych osobowych								
Cele przedmiotu	Celem przedmiotu jest zapoznanie z wymogami prawa ochrony danych osobowych w związku z tworzeniem i wdrażaniem systemu ochrony danych osobowych w organizacji.								
Treści programowe	Wykład: organizacja ochrony danych osobowych. Administrator bezpieczeństwa informacji. Filary zgodnego z prawem przetwarzania danych osobowych – obowiązki administratora danych. Ćwiczenia: organizacyjne środki ochrony danych osobowych. Techniczne środki ochrony danych osobowych. Uprawnienia UODO oraz odpowiedzialność za naruszenie przepisów o ochronie danych osobowych.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz charakteryzuje zasady tworzenia i wdrażania systemu ochrony danych osobowych w organizacji.							ZBI_W3	
EU2	Słuchacz wskazuje wymagania przepisów prawa ochrony danych osobowych.							ZBI_W3	
EU3	Słuchacz wdraża wybrane elementy systemu ochrony danych osobowych w dowolnej jednostce organizacyjnej, oraz analizuje i ocenia system ochrony danych osobowych.							ZBI_U3	
EU4	Słuchacz komunikuje się prawidłowo używając terminologii wewnętrznej i zewnętrznej w ramach systemu ochrony danych osobowych oraz współdziała							ZBI_U8	

	w grupie na potrzeby wdrażania systemu ochrony danych osobowych.	
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja
EU1	zaliczenie ustne	W
EU2	zaliczenie ustne	W
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.
Wyliczenie	udział w wykładach	4
	udział w ćwiczeniach	4
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	10
	przygotowanie do zaliczenia ustnego z wykładu	6
	RAZEM:	25
Wskaźniki ilościowe		GODZINY ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		9 0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		15 0,6
Literatura podstawowa	1. Gałąj-Emiliańczyk K., Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku, Difin S.A., Warszawa 2016. 2. Gawroński M., Ochrona danych osobowych: przewodnik po ustawie i RODO z wzorami, Wolters Kluwer, Warszawa 2018. 3. Banyś T., Łuczak J., Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, PRESSCOM, Wrocław 2017.	
Literatura uzupełniająca	1. Kępa L., Ochrona danych osobowych w praktyce, Difin S.A., Warszawa 2015.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	mgr Konrad Gałąj-Emiliańczyk	15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Informatyka śledcza z elementami hackingu - metody i środki ochrony danych							Kod przedmiotu	SPZBI10
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	2
	8	8						Punkty ECTS	3
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest charakterystyka nośników oraz właściwości danych informatycznych ze szczególnym uwzględnieniem sposobów zachowania ich integralności, poufności i dostępności.								
Treści programowe	Wykład: dowody elektroniczne, sposoby ich zabezpieczania, retencja dowodów drzemiących oraz ich istotność w sprawie. Pojęcie i istota łańcucha dowodowego. Ćwiczenia: praktyczne metody i narzędzia odzyskiwania danych skasowanych z nośników pamięci i urządzeń mobilnych GSM. Wewnętrzny audyt informatyczny w organizacji. Testy penetracyjne usprawniające proces zabezpieczenia danych w organizacji. Etapy przygotowania projektu w zakresie wdrożenia systemów teleinformatycznych w organizacji.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz wymienia atrybuty dowodu elektronicznego oraz wskazuje istotę łańcucha dowodowego.							ZBI_W5	
EU2	Słuchacz charakteryzuje i stosuje najważniejsze narzędzia wykorzystywane w informatyce śledczej.							ZBI_W5, ZBI_U5	
EU3	Słuchacz wymienia i charakteryzuje obszary i cele audytu informatycznego oraz testów penetracyjnych.							ZBI_W5	
EU4	Słuchacz przygotowuje projekt i planuje realizację inwestycji w obszarze teleinformatyki.							ZBI_U1, ZBI_U5	

Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja	
EU1	zaliczenie ustne	W	
EU2	zaliczenie ustne (W), ocena rozwiązywania praktycznego problemu w trakcie zajęć (C)	W, C	
EU3	zaliczenie ustne	W	
EU4	ocena rozwiązywania praktycznego problemu w trakcie zajęć	C	
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.	
Wyliczenie	udział w wykładach	8	
	udział w ćwiczeniach	8	
	udział w konsultacjach	2	
	wykonanie indywidualnych zadań ćwiczeniowych	16	
	samodzielne studia literatury przedmiotu	24	
	przygotowanie do zaliczenia ustnego z wykładu	17	
	RAZEM:	75	
Wskaźniki ilościowe		GODZINY	ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		18	0,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		50	2
Literatura podstawowa	1. Carvey H., Altheide C., Informatyka śledcza, Przewodnik po narzędziach open source, Wydawnictwo Helion, Gliwice 2014. 2. Brzozowska M., Przygotowanie do RODO w IT, Wrocław 2018. 3. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. 1997, nr 88, poz. 553 z późn. zm.).		
Literatura uzupełniająca	1. Kowalewski J., Kowalewski M., Zagrożenia informacji w cyberprzestrzeni, cyberterrorizm, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017. 2. Listkiewicz J., Listkiewicz S., Niedziółka D., Szymczak P., Metody realizacji projektów inwestycyjnych planowanie, finansowanie, ocena, Ośrodek Doradztwa i Doskonalenia Kadr, Warszawa 2004.		
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu	
Program opracował(a)	mgr Dariusz Gromadka	15.01.2019	

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Ochrona danych osobowych w przedsiębiorstwie i administracji publicznej - studia przypadków							Kod przedmiotu	SPZBI11
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	2
	8	8						Punkty ECTS	3
Przedmioty wprowadzające	Międzynarodowe i krajowe regulacje prawne w zakresie ochrony danych osobowych								
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy się ze specyfiką zarządzania bezpieczeństwem i ciągłością informacji w organizacjach sektora prywatnego i publicznego na podstawie przykładów z doświadczenia prowadzącej, decyzji Urzędu Ochrony Danych Osobowych (UODO) oraz orzecznictwa.								
Treści programowe	Wykład: zarządzanie ciągłością i bezpieczeństwem informacji w organizacji. Ochrona danych osobowych oraz innych informacji chronionych w urzędzie, bibliotece, spółce akcyjnej, agencji reklamowej, małej firmie. Ćwiczenia: problemy związane z dostępem do informacji publicznej. Problemy rozdziału kwestii ochrony danych osobowych od kwestii bezpieczeństwa informacji. Brak komunikacji w organizacji – największe zagrożenie dla bezpieczeństwa informacji chronionych. Niewiedza personelu – punkt wyjścia do większości incydentów. Najgroźniejsze incydenty – przyczyny oraz konsekwencje.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, studia przypadków, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz charakteryzuje zakres funkcjonowania systemu zarządzania bezpieczeństwem informacji w organizacji sektora prywatnego i publicznego.							ZBI_W3	
EU2	Słuchacz rozwiązuje praktyczne problemy w zakresie ochrony informacji.							ZBI_U3	
EU3	Słuchacz stosuje odpowiednie środki zaradcze dla naruszeń bezpieczeństwa danych.							ZBI_U4	
EU4	Słuchacz planuje, organizuje oraz nadzoruje proces							ZBI_U3, ZBI_K3	

	bezpieczeństwa danych osobowych z zachowaniem zasad etyki zawodowej Inspektora Ochrony Danych.		
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja	
EU1	zaliczenie ustne	W	
EU2	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
Bilans nakładu pracy studenta (w godzinach)			Liczba godz.
Wyliczenie	udział w wykładach	8	
	udział w ćwiczeniach	8	
	udział w konsultacjach	1	
	wykonanie indywidualnych zadań ćwiczeniowych	15	
	samodzielne studia literatury przedmiotu	23	
	przygotowanie do zaliczenia ustnego z wykładu	20	
	RAZEM:	75	
Wskaźniki ilościowe			GODZINY
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela			ECTS
			17
			0,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym			47
			1,9
Literatura podstawowa	1. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa -Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018. 2. Lubasz D., RODO: zmiany w zakresie ochrony danych osobowych: porównanie przepisów, praktyczne uwagi, Wolters Kluwer, Warszawa 2018. 3. Czub-Kielczewska S., ABC ochrony danych osobowych w bibliotece, Medialex 2016.		
Literatura uzupełniająca	1. Strona internetowa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl		
Jednostka realizująca	Wydział Inżynierii Zarządzania PB		Data opracowania programu
Program opracował(a)	mgr Sylwia Czub-Kielczewska		15.01.2019

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Etyka zawodowa w zarządzaniu informacją							Kod przedmiotu	SPZBI12
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	2
	4	4						Punkty ECTS	1
Przedmioty wprowadzające	-								
Cele przedmiotu	Celem przedmiotu jest przekazanie wiedzy i kształtowanie praktycznych umiejętności analizy etycznej oraz kompetencji rozwiązywania dylematów etycznych w organizacji.								
Treści programowe	Wykład: geneza i źródła etyki. Człowiek i jego wartości. Dylematy moralne w podejmowaniu decyzji. Etyczne modele decyzyjne oraz dylematy etyczne wybranych grup zawodowych. Etyka menedżera. Ćwiczenia: etyka „nieetyczna”, czyli ambiwalencje etyki. Instytucja whistle-blowing - informowanie – donoszenie. Prywatność w firmie. Przykłady łamania prywatności pracowników w firmach w Polsce i na świecie. Sytuacje konfliktowe. Patologie „etyki”.								
Metody dydaktyczne	wykład problemowy, studia przypadku, burza mózgów, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz wymienia i charakteryzuje najważniejsze teorie etyczne.							ZBI_W6	
EU2	Słuchacz analizuje problem etyczny. Rozstrzyga dylematy etyczne w oparciu o poznane teorie.							ZBI_U6	
EU3	Słuchacz analizuje uwarunkowania dysfunkcyjnych zjawisk i zachowań w organizacji.							ZBI_W6, ZBI_U6	
EU4	Słuchacz opisuje proces podejmowania etycznej decyzji w organizacji. Określa sposób rozwiązania sytuacji konfliktowej w trakcie pełnienia roli Inspektora Ochrony Danych.							ZBI_W6, ZBI_K3	

Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja		
EU1	zaliczenie ustne	W		
EU2	ocena rozwiązania praktycznego problemu w trakcie zajęć	C		
EU3	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C		
EU4	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C		
Bilans nakładu pracy studenta (w godzinach)			Liczba godz.	
Wyliczenie	udział w wykładach	4		
	udział w ćwiczeniach	4		
	udział w konsultacjach	1		
	wykonanie indywidualnych zadań ćwiczeniowych	8		
	przygotowanie do zaliczenia ustnego z wykładu	8		
	RAZEM:	25		
Wskaźniki ilościowe			GODZINY	ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela			9	0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym			13	0,5
Literatura podstawowa	1. Gasparski W., Dielt J., Etyka biznesu, PWN, Warszawa 2000. 2. Lewicka-Strzalecka A., Etyczne standardy firm i pracowników, IFIS PAN, Warszawa 1999.			
Literatura uzupełniająca	1. Czerkawska A., Czerkawski A., Etyczny wymiar poradnictwa zawodowego, KOWEziU, Warszawa 2005. 2. Deutsch M., Coleman P. T., Rozwiązywanie konfliktów. Teoria i praktyka, Wydawnictwo Uniwersytetu Jagiellońskiego Wydawnictwo, Kraków 2005.			
Jednostka realizująca	Wydział Inżynierii Zarządzania PB		Data opracowania programu	
Program opracował(a)	dr Joanna Szydło		15.01.2019	

Wydział Inżynierii Zarządzania									
Kierunek studiów	Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych							Poziom i forma studiów	studia podyplomowe
Specjalność / ścieżka dyplomowania								Profil kształcenia	
Nazwa przedmiotu	Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017							Kod przedmiotu	SPZBI13
								Rodzaj przedmiotu	obowiązkowy
Formy zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	Semestr	2
	12	12						Punkty ECTS	3
Przedmioty wprowadzające	Normy bezpieczeństwa i ochrona informacji w organizacji								
Cele przedmiotu	Celem przedmiotu jest zdobycie umiejętności i wiedzy potrzebnej do prowadzenia audytów wewnętrznych systemu zarządzania bezpieczeństwem informacji (SZBI) ISO/IEC 27001:2017.								
Treści programowe	Wykład: wprowadzenie do bezpieczeństwa informacji. Omówienie wymagań normy ISO/IEC 27001:2017 pod kątem audytowania. Kompetencje oraz rola audytorów wewnętrznych. Wytyczne dotyczące audytowania - wymagania ISO 19011:2011. Ćwiczenia: planowanie audytów wewnętrznych. Przygotowanie do audytu. Prowadzenie działań audytowych. Dokumentowanie audytu. Raportowanie z audytu. Komunikacja werbalna i niewerbalna w audycie. Praktyczne zadania z zakresu audytowania.								
Metody dydaktyczne	wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie								
Forma zaliczenia	wykład – egzamin pisemny; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć								
Symbol efektu uczenia się	Zakładane efekty uczenia się							Odniesienie do kierunkowych efektów uczenia się	
EU1	Słuchacz charakteryzuje zakres normy ISO/IEC 27001:2017.							ZBI_W3	
EU2	Słuchacz wskazuje wymagania przepisów w zakresie normy ISO/IEC 27001:2017.							ZBI_W3	
EU3	Słuchacz prowadzi audyty wewnętrzne SZBI.							ZBI_U7	
EU4	Słuchacz poprawnie dostosowuje swoje postępowanie z zachowaniem zasad etyki zawodowej w odniesieniu do trudnej sytuacji w trakcie prowadzenia audytu oraz krytycznie oceniając posiadaną wiedzę umiejętnie							ZBI_K2, ZBI_K3, ZBI_U9	

	dobiera szkolenia umożliwiającego rozwój zawodowy własny i pracowników mu podległych.		
Symbol efektu uczenia się	Sposoby weryfikacji efektów uczenia się	Forma zajęć, na której zachodzi weryfikacja	
EU1	egzamin pisemny	W	
EU2	egzamin pisemny	W	
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
EU4	ocena rozwiązania praktycznego problemu w trakcie zajęć	C	
Bilans nakładu pracy studenta (w godzinach)		Liczba godz.	
Wyliczenie	udział w wykładach	12	
	udział w ćwiczeniach	12	
	udział w konsultacjach	1	
	wykonanie indywidualnych zadań ćwiczeniowych	20	
	samodzielne studia literatury przedmiotu	15	
	przygotowanie do egzaminu pisemnego z wykładu	15	
	RAZEM:	75	
Wskaźniki ilościowe		GODZINY	ECTS
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		25	1
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		48	1,9
Literatura podstawowa	1. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa -Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018. 2. Wytyczne dotyczące auditowania systemów zarządzania: PN-EN ISO 19011. Warszawa: Polski Komitet Normalizacyjny, 2012. 3. Polaczek T. Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice 2006.		
Literatura uzupełniająca	1. Łukacz J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Poznań 2009, https://jacekluczak.pl/images/download/Systemowe.pdf		
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu	
Program opracował(a)	dr inż. Dariusz Kłosowski, inż. Krzysztof Smogorzewski	15.01.2019	

ZASOBY BIBLIOTECZNE ORAZ ELEKTRONICZNE ZASOBY WIEDZY OBEJMUJĄCE LITERATURĘ ZALECANĄ NA STUDIACH PODYPLOMOWYCH ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – INSPEKTOR OCHRONY DANYCH, DO KTÓRYCH UCZELNIA ZAPEWNIĄ DOSTĘP

Biblioteka Politechniki Białostockiej zapewnia dostęp do zasobów bibliotecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną na Studiach Podyplomowych Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych.

Biblioteka Politechniki Białostockiej jest największą biblioteką naukowo-techniczną w regionie północno-wschodnim Polski. Biblioteka PB jest podstawą systemu biblioteczno-informacyjnego uczelni. W jej skład wchodzi Biblioteka Główna oraz Biblioteka Wydziału Architektury, Biblioteka Wydziału Inżynierii Zarządzania oraz Biblioteka Zamiejscowego Wydziału Leśnego w Hajnówce. Zadaniem Biblioteki Głównej jest zaspokajanie potrzeb wszystkich pracowników i studentów w zakresie dostępu do literatury naukowej i dydaktycznej. Biblioteki specjalistyczne obsługują zaś poszczególne jednostki organizacyjne uczelni (wydziały, instytuty) gromadzą i udostępniają księgozbiór ściśle związany z ich potrzebami.

Władze i nauczyciele akademicy Wydziału Inżynierii Zarządzania PB współpracują ściśle z Biblioteką PB w zakresie bieżącego gromadzenia zbiorów (książek oraz czasopism krajowych i zagranicznych), z wyspecjalizowanymi dokumentami włącznie. W procesie powiększania zbiorów uwzględniane są także potrzeby z zakresu zarządzania bezpieczeństwem informacji, który jest skorelowany z realizowanymi kierunkami studiów. Bieżące zakupy krajowych i zagranicznych wydawnictw naukowych zapewniają dostęp studentom i nauczycielom akademickim Wydziału Inżynierii Zarządzania do najnowszej literatury specjalistycznej.

Od 1951 roku Biblioteka PB zgromadziła ponad 406 tysięcy książek, czasopism, norm i literatury firmowej. Tematyka księgozbioru jest ściśle związana z potrzebami wydziałów i kierunkami studiów Politechniki Białostockiej. Wśród zgromadzonych materiałów bibliotecznych ważne miejsce zajmują wydawnictwa z zakresu: mechaniki; budowy, eksploatacji i technologii maszyn; biocybernetyki i inżynierii biomedycznej; automatyki i robotyki; elektrotechniki, elektroniki i telekomunikacji; informatyki; budownictwa; inżynierii i ochrony środowiska; zarządzania i marketingu; architektury; nauk matematyczno-przyrodniczych.

Tabela 1. Zbiory Biblioteki Politechniki Białostockiej w rozbiciu na kategorie

Lp.	Opis	Stan na 31.12.2017
	Łącznie zasoby (liczba woluminów), w tym:	406 331
1.	wydawnictwa zwarte	281 495
	wydawnictwa ciągłe	45 907
	zbiory specjalne (normy, literatura firmowa, dokumenty elektroniczne)	78 929
	Liczba czasopism prenumerowanych (dostępnych w formie papierowej), w tym:	419
2.	wydawnictwa polskie	389
	wydawnictwa zagraniczne	30
	Liczba wydawnictw zarejestrowanych (liczba woluminów), w tym:	6 821
3.	wydawnictwa zwarte	6 164
	wydawnictwa ciągłe	546
	zbiory specjalne (normy, literatura firmowa, dokumenty elektroniczne)	111

Źródło: dane z Biblioteki Głównej Politechniki Białostockiej.

Od 1995 roku w Bibliotece PB działa niezawodnie zintegrowany system biblioteczny ALEPH. Uruchomiona w 2009 roku 18 wersja ALEPH 500 zapewnia użytkownikom przyjazne środowisko pracy. Umożliwia korzystanie z nowych usług, np. automatycznej komunikacji za pomocą poczty elektronicznej dotyczącej wypożyczenia książek oraz przesyłania zestawień tematycznych, a pracownikom biblioteki oferuje wiele nowych funkcji ułatwiających wprowadzanie danych. Zarejestrowani użytkownicy mogą zdalnie zamawiać książki, prolongować terminy ich zwrotu oraz kontrolować stan swojego konta. Obecnie wszystkie zbiory biblioteczne są widoczne w katalogu online.

Od października 2012 roku Biblioteka Główna funkcjonuje w gmachu Centrum Nowoczesnego Kształcenia. W nowoczesnych pomieszczeniach udostępniane są połączone zbiory Biblioteki Głównej oraz funkcjonujących dawniej bibliotek wydziałowych zlokalizowanych na terenie kampusu. Zgromadzenie w jednym miejscu bogatego księgozbioru pozwoliło na wyodrębnienie, na trzech kondygnacjach budynku, ogólnodostępnych, specjalistycznych czytelni:

- Czytelnia Wydawnictw Informacyjnych - 27 miejsc;
- Czytelnia Elektroniczna - 24 miejsca;
- Czytelnia Czasopism - 24 miejsca;
- Czytelnia Norm i Zbiorów Specjalnych - 10 miejsc;
- Czytelnia Książek - 81 miejsc.

Użytkownicy mogą korzystać również z 19 specjalnie zaprojektowanych i wyposażonych pomieszczeń do pracy indywidualnej i zbiorowej (72 miejsca). Dodatkowo na potrzeby szkoleń, prezentacji czy ćwiczeń dostępna jest sala multimedialna, w której są 32 stanowiska komputerowe. Łącznie Biblioteka PB dysponuje 378 miejscami dla czytelników (Biblioteka Główna - 270 oraz biblioteki specjalistyczne – 108). W 2015 roku na terenie Czytelni Książek utworzono stanowisko do pracy dla osób niepełnosprawnych ze specjalistycznym oprogramowaniem komputerowym.

Ponadto do dyspozycji użytkowników jest 108 stanowisk komputerowych z dostępem do Internetu. Na wybranych stanowiskach zainstalowano specjalistyczne oprogramowanie: Adobe AfterEffects CS6, Adobe Design & Web Premium CS6 (Photoshop, Illustrator, InDesign, Dreamweaver, Flash Professional, Fireworks, Acrobat X Pro, Bridge, Media Encoder), Adobe Photoshop CS6 Extended, Altium Designer 10 Academic, Android Studio, ArchiCAD 20 oraz 19, Autodesk Education Master Suite 2014 EDU (AutoCAD, Autodesk), Blender, Code Blocks Studio, Corel Designer Technical Suite X5, CorelDRAW Graphics Suite X6 (CorelDRAW, PHOTO-PAINT, PowerTRACE, CAPTURE, CONNECT), Dev-C++ , Embarcadero RAD Studio XE2 Professional (Delphi XE2, C++Builder XE2, Embarcadero Prism XE2, RadPHP XE2 & Android Platform, InterBase XE Developer Edition), Flash Builder Premium 4.5, GIMP, Microsoft Office 2010 oraz 2003, MikroMap, Netbeans IDE, Norma PRO EDU, proTeXtorazLEd - LaTeXEdytor, Solid Works 2017, Statistica 13.1, University Bundle V-Ray 2.0 for 3ds Max EDU + Pdplayer, Vensim PLE, Visual Studio Express 2012, WinKalk.

Użytkownicy mogą także korzystać z wysokiej klasy samoobsługowych skanerów (3 znajdują się w Bibliotece Głównej, 1 – w Bibliotece Wydziału Inżynierii Zarządzania) oraz skanerów płaskich dostępnych przy stanowiskach komputerowych.

Wychodząc naprzeciw potrzebom czytelników Biblioteka wprowadziła szereg rozwiązań podnoszących jakość świadczonych usług i komfort korzystania ze zbiorów. Przede wszystkim wolny, swobodny dostęp do najnowszych zbiorów naukowych i dydaktycznych. Regulaminy czytelni zarówno Biblioteki Głównej jak i bibliotek specjalistycznych uwzględniają krótkoterminowe wypożyczenia zbiorów poza

obręb czytelnik na okres 7 dni lub na 3 godziny. Specjalne urządzenia (self-checki) pozwalają na samodzielne wypożyczenia i zwroty książek. Zamontowane na zewnątrz budynku CNK urządzenie „wrzutnia” umożliwia również zwrot książek w czasie zamknięcia biblioteki.

Istotnym uzupełnieniem księgozbioru bibliotecznego są zasoby elektroniczne. Dostęp do najnowszych osiągnięć nauki zapewniają tematyczne i wielod dziedzinowe serwisy czasopism i książek elektronicznych. Biblioteka PB oferuje dostęp do następujących baz danych:

baz pełnotekstowych, m.in.:

- EBSCOhost (serwis interdyscyplinarny);
- Elsevier (baza interdyscyplinarna ScienceDirect);
- Emerald Engineering and Emerald Management Journals (automatyka, robotyka, matematyka obliczeniowa, elektronika, inżynieria materiałowa, zarządzanie, marketing, finanse, logistyka, technika);
- Emerging Markets Information Service (EMIS) (biznes, zarządzanie i rachunkowość, ekonomia i finanse);
- IBUK libra (baza interdyscyplinarna książek polskich);
- IEEE Xplore Digital Library (technika);
- INFONA (interdyscyplinarna);
- Knovel Library (technika);
- Naukowa Akademicka Sieciowa Biblioteka Internetowa (NASBI) (baza interdyscyplinarna książek polskich);
- OECD iLibrary (interdyscyplinarna);
- ProQuest Ebook Central (interdyscyplinarna);
- SPRINGER (interdyscyplinarna);
- Wiley Online Library (interdyscyplinarna).

baz bibliograficzno-abstraktowych:

- ISI Web of Science (interdyscyplinarna);
- MathSciNet (matematyka, informatyka i dziedziny pokrewne);
- Scopus (interdyscyplinarna);
- Web of Science (interdyscyplinarna);

indywidualnych tytułów czasopism, m.in.:

- Building Services Engineering Research & Technology;
- Computer Methods in Material Science;
- Géotechnique;
- Journal of Landscape Architecture;
- LEUKOS;

- Lighting Research and Technology;
- Miesięcznik Hotelarz;
- Miesięcznik Rynek Turystyczny;
- Nature Publishing Group (interdyscyplinarna);
- Poradnik gospodarowania odpadami on-line;
- Science (nauki przyrodnicze i inne);
- Vademecum Bibliotekarza on-line.

oraz krajowych i zagranicznych baz ogólnodostępnych, jak:

- AGRO (nauki przyrodnicze, rolnicze i techniczne);
- BazEkon (ekonomia);
- BazTech (nauki techniczne oraz w wyborze nauki ścisłe i ochrona środowiska);
- Directory of Open Access Journals (multidyscyplinarna);
- ElektronischeZeitschriftenbibliothek (multidyscyplinarna).

W 2016 roku Biblioteka PB uruchomiła wyszukiwarkę naukową PRIMO – nowoczesne i uniwersalne narzędzie, służące do jednoczesnego przeszukiwania wszystkich zasobów bibliotecznych, zarówno tradycyjnych jak i elektronicznych. Dzięki niej przeszukiwanie zbiorów jest bardzo proste. Jedno okno wyszukiwawcze pozwala szybko i efektywnie dotrzeć do wszystkich lokalnych oraz zdalnych zasobów, a wyniki są pogrupowane wg indywidualnych potrzeb czytelnika.

W 2004 roku zostało zawarte „Porozumienie o utworzeniu Konsorcjum Bibliotek Naukowych Miasta Białegostoku”. W ramach tego porozumienia w 2006 r. rozpoczęła działalność Podlaska Biblioteka Cyfrowa (dalej PBC). Biblioteka PB aktywnie uczestniczy w tworzeniu zasobu edukacyjnego poprzez rozwój Kolekcji Naukowo-Dydaktycznej. W jej skład wchodzi podręczniki dla studentów, monografie, skrypty i artykuły naukowe autorstwa pracowników Politechniki Białostockiej, w tym pracowników Wydziału Inżynierii Zarządzania. W 2017 roku Biblioteka Politechniki Białostockiej zdigitalizowała 22 nowych publikacji, co łącznie daje 284 pozycje w zasobie PBC. Materiały te cieszą się dużym zainteresowaniem i zajmują czołowe miejsca wśród najbardziej poczytnych pozycji. W 2016 roku zarejestrowano 84 tys. wyświetleń publikacji zgromadzonych w PBC, a w 2017 roku było ich blisko 94 tys.

Na Wydziale Inżynierii Zarządzania PB funkcjonuje Biblioteka Wydziału Inżynierii Zarządzania (czytelnia i wypożyczalnia), będąca częścią systemu biblioteczno-informacyjnego Politechniki Białostockiej. Biblioteka zajmuje powierzchnię 248 m². Zlokalizowana jest na parterze jednego z głównych budynków Wydziału, z łatwym dostępem dla osób niepełnosprawnych. Pomieszczenia biblioteki składają się z czytelni oraz dwóch magazynów, w których zastosowano magazynowanie zwarte (regaly jezdne). W czytelni użytkownicy mają do dyspozycji:

- 30 miejsc do pracy indywidualnej cichej;
- wolny dostęp do ok. 6.300 zbiorów ułożonych według różnych działów wiedzy (32 regaly);
- wolny dostęp do wszystkich bieżących (5 regalów) i niektórych archiwalnych numerów czasopism i gazet (8 regalów);

- 7 stanowisk komputerowych z dostępem do bibliotecznego systemu ALEPH i Internetu;
- skaner samoobsługowy Zeta Zeutschel.

Oprócz tego, w 2013 roku wydzielono z części magazynowej i udostępniono czytelnikom osobne pomieszczenie do pracy grupowej dla max. 8 osób. Ponadto, w całej bibliotece oferowany jest dostęp do Internetu bezprzewodowego, który umożliwia korzystanie z własnych urządzeń przenośnych. Ta forma korzystania z zasobów sieci cieszy się bardzo dużym powodzeniem.

Zasoby biblioteczne są stale aktualizowane i wzbogacane z uwzględnieniem potrzeb nauczycieli akademickich i studentów Wydziału Inżynierii Zarządzania. Władze i nauczyciele akademicy Wydziału współpracują ściśle z biblioteką w zakresie bieżącego gromadzenia zbiorów tradycyjnych i elektronicznych. Dotyczy to zarówno wydawnictw zwartych, prenumeraty czasopism w wersji papierowej i elektronicznej, dostępu do elektronicznych baz danych. Biblioteka Wydziału Inżynierii Zarządzania gromadzi i udostępnia literaturę związaną ściśle z kierunkami kształcenia prowadzonymi na Wydziale, a także realizowanymi badaniami naukowymi.

Biblioteka Wydziału Inżynierii Zarządzania corocznie kupuje do swoich zbiorów ok. 1000-1500 wol. książek, z czego ok. 100-200 kupowanych jest przez nauczycieli akademickich w ramach grantów otrzymanych na badania naukowe. Do biblioteki wpływają także materiały konferencyjne przekazywane przez pracowników Wydziału uczestniczących w konferencjach krajowych i zagranicznych oraz starannie dobierane dary pochodzące od osób prywatnych i instytucji. Liczba zbiorów pozyskiwanych z tego źródła wpływu wynosi ok. 150-200 wol. rocznie.

Biblioteka Politechniki Białostockiej zapewnia dostęp między innymi do następujących zasobów bibliecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną na Studiach Podyplomowych Zarządzanie Bezpieczeństwem Informacji – Inspektor Ochrony Danych:

zasoby biblieczne:

1. Bandyś T.A.J. i in., Prawo ochrony danych osobowych: podręcznik dla studentów i praktyków. Difin, Warszawa, 2016.
2. Banyś T., Łuczak J., Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, PRESSCOM, Wrocław 2017.
3. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017.
4. Brzozowska M., Przygotowanie do RODO w IT, Wrocław 2018.
5. Carvey H., Altheide C., Informatyka śledcza, Przewodnik po narzędziach open source, Wydawnictwo Helion, Gliwice 2014.
6. Czub-Kielczewska S., ABC ochrony danych osobowych w bibliotece, Medialex 2016.
7. Domagała M. i in., Nowe standardy w ochronie danych osobowych, Wydawnictwo Think & Make, Warszawa 2018.
8. Gałaj-Emiliańczyk K., Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku, Difin S.A., Warszawa 2016.
9. Gasparski W., Dietl J., Etyka biznesu, PWN, Warszawa 2000.
10. Gawroński M., Ochrona danych osobowych: przewodnik po ustawie i RODO z wzorami, Wolters Kluwer, Warszawa 2018.
11. Kaczmarek T.T., Zarządzanie ryzykiem: ujęcie interdyscyplinarne, Difin, Warszawa 2010.

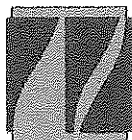
12. Kowalewski J., Kowalewski M., Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017.
13. Kuc B.R., Moczydłowska J.M., Zachowania organizacyjne, Difin 2009.
14. Lewicka-Strzałecka A., Etyczne standardy firm i pracowników, IFiS PAN, Warszawa 1999.
15. Lubasz D., RODO: zmiany w zakresie ochrony danych osobowych: porównanie przepisów, praktyczne uwagi, Wolters Kluwer, Warszawa 2018.
16. Moczydłowska J.M., Kowalewski K., Nowe koncepcje zarządzania ludźmi, Difin 2014.
17. Moczydłowska J.M., Serafin K., Doskonalenie kompetencji zawodowych w profesjonalnie zarządzanej organizacji, Wydawnictwo Naukowe Sophia, Katowice 2016.
18. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018.
19. PN-ISO/IEC 27002:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji, wyd. PKN, Warszawa 2018.
20. PN-ISO/IEC 27005:2014-01, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014.
21. Sitaniec I., Zawila-Niedźwiecki J. (red.), Ryzyko operacyjne w naukach o zarządzaniu, C.H. Beck, Warszawa 2015.
22. Wytyczne dotyczące auditowania systemów zarządzania: PN-EN ISO 19011. Warszawa: Polski Komitet Normalizacyjny, 2012.

elektroniczne zasoby wiedzy:

1. Jatkiewicz P., Uwarunkowania zarządzania systemem bezpieczeństwa informacji w jednostkach samorządu terytorialnego, Uniwersytet Gdański, Wydział Zarządzania, Gdańsk 2012.
2. Konstytucja RP z dnia 2 kwietnia 1997 r.
3. Łukacz J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Poznań 2009, <https://jacekluczak.pl/images/download/Systemowe.pdf>
4. Moczydłowska J.M., Paradoxy w zarządzaniu kapitałem ludzkim w ocenie menedżerów, „Nauki o Zarządzaniu” 2016, nr 2 (27), s. 130-138.
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)
6. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948).
7. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. 2011, nr 156, poz. 926).
8. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011, nr 288, poz. 1692).
9. Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. 2011, nr 93, poz. 541).

10. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa, w sprawie wzoru decyzji o odmowie poświadczenia bezpieczeństwa osobowego (Dz.U. 2010, nr 258, poz. 1752).
11. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz.U. 2017, poz. 2334).
12. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. 2012, poz. 683).
13. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011, nr 276, poz. 1631).
14. Strona internetowa Urzędu Ochrony Danych Osobowych, <https://uodo.gov.pl>
15. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
16. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. 2018, poz. 2096).
17. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 1993, nr 47, poz. 211 z późn. zm.).
18. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, Nr 182, poz. 1228 z późn. zm.).
19. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. 1997, nr 88, poz. 553 z późn. zm.).
20. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001, nr 1497, poz. 229 z późn.zm.).

**OPINIA WYDZIAŁOWEJ KOMISJI DS. JAKOŚCI KSZTAŁCENIA WYDZIAŁU INŻYNIERII
ZARZĄDZANIA DOTYCZĄCA PROGRAMU STUDIÓW PODYPLOMOWYCH ZARZĄDZANIE
BEZPIECZEŃSTWEM INFORMACJI – INSPEKTOR OCHRONY DANYCH**



**Wydział Inżynierii Zarządzania
Politechniki Białostockiej**

ul. Ojca Tarasiuka 2, 16-001 Kleosin, e-mail: wiz_sekretariat@pb.edu.pl, tel. +48 85 746 98 02

Białystok, 05 luty 2019r.

Opinia

Na posiedzeniu WK ds. JK przeanalizowała program studiów podyplomowych „Zarządzanie Bezpieczeństwem Informacji - Inspektor Ochrony Danych”.

Przedstawiony program studiów został wcześniej rozesłany mailem do członków WK ds. JK. Członkowie Komisji przedstawili autorom uwagi dotyczące programu studiów. Na zebraniu członkowie komisji potwierdzili, że przedstawione uwagi zostały wypełnione. W wyniku przeprowadzonej dyskusji stwierdzono, że przedstawiony program studiów podyplomowych „Zarządzanie Bezpieczeństwem Informacji - Inspektor Ochrony Danych” jest bardzo aktualny i postanowiono pozytywnie go zaopiniować.

Przewodniczący WK ds. JK
Przewodniczący Wydziałowej Komisji
ds. Jakości Kształcenia
Wydziału Inżynierii Zarządzania
dr inż. Arkadiusz Lukjaniuk

**UCHWAŁA NR 9/2/2019 RADY WYDZIAŁU INŻYNIERII ZARZĄDZANIA Z DNIA 06.02.2019 R.
W SPRAWIE URUCHOMIENIA STUDIÓW PODYPLOMOWYCH: ZARZĄDZANIE
BEZPIECZEŃSTWEM INFORMACJI - INSPEKTOR OCHRONY DANYCH II EDYCJA I POWOŁANIA
KIEROWNIKA TYCH STUDIÓW**

**Uchwała nr 9./2/2019
Rady Wydziału Inżynierii Zarządzania**

z dnia 6 lutego 2019 roku

**w sprawie uruchomienia studiów podyplomowych: Zarządzanie Bezpieczeństwem
Informacji - Inspektor Ochrony Danych II edycja
i powołania kierownika tych studiów**

Na podstawie § 58 pkt. 1, ppkt. 6 Statutu Politechniki Białostockiej oraz § 2 Regulaminu Studiów Podyplomowych Rada Wydziału Inżynierii Zarządzania postanawia:

§ 1

1. Uruchomić w roku akademickim 2018/2019 studia podyplomowe: **Zarządzanie Bezpieczeństwem Informacji - Inspektor Ochrony Danych II edycja.**
2. Pozytywnie zaopiniować powołanie na kierownika tych studiów dr Danuty Szpilko.


§ 2

Zatwierdzić plany i programy studiów określonych w § 1.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Obradom Rady Wydziału Inżynierii
Zarządzania przewodniczyła

DZIEKAN
WYDZIAŁU INŻYNIERII ZARZĄDZANIA
Politechniki Białostockiej

dr hab. inż. Jolanta Wójciszka, prof. nzw.