UCHWAŁA NR 414 /XXIV/XV/2019
Senatu Politechniki Białostockiej
z dnia 18 kwietnia 2019 roku

- w sprawie ustalenia programu studiów podyplomowych Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji

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 Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji, stanowiący załącznik do niniejszej uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

REKTOR

prof. dr hab. inż. Lech Dzienis

Załącznik do Uchwały Nr 414/XXIV/XV/2019 Senatu PB

WYDZIAŁ INŻYNIERII ZARZĄDZANIA
POLITECHNIKI BIAŁOSTOCKIEJ

PROGRAM STUDIÓW PODYPLOMOWYCH

MENEDŻER DS. BEZPIECZEŃSTWA INFORMATYCZNEGO I RYZYKA W OCHRONIE INFORMACJI

Białystok, 2019 r.

P.O. KIEROWNIK
SEKCJI JAKOŚCI KSZTAŁCENIA
Politechniki Białostockiej
dr inż. Joanna Krętowska

PROREKTOR
ds. Kształcenia i Współpracy Międzynarodowej
dr hab. inż. Maria Kosiur Kozbiel, prof. PB

DZIEKAN
WYDZIAŁU INŻYNIERII ZARZĄDZANIA
Politechniki Białostockiej
dr hab. inż. Joanna Ejdys, prof. PB

PROGRAM STUDIÓW PODYPLOMOWYCH
MENEDŻER DS. BEZPIECZEŃSTWA INFORMATYCZNEGO I RYZYKA W OCHRONIE INFORMACJI

Studia podyplomowe Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji trwają 2 semestry i umożliwiają uzyskanie kwalifikacji cząstkowych na poziomie 6 PRK. Łączna liczba punktów ECTS: 30. Łączna liczba godzin zajęć: 160.

Plan studiów
MENEDŻER DS. BEZPIECZEŃSTWA INFORMATYCZNEGO I RYZYKA W OCHRONIE INFORMACJI

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.	Zarządzanie ryzykiem w bezpieczeństwie informacji	8	8	16	3	E
2.	Szacowanie ryzyka w ochronie danych osobowych	8	8	16	3	ZO
3.	Systemy informatyczne wspomagające ochronę informacji	12	12	24	4	ZO
4.	Zarządzanie incydentami w ochronie informacji	8	8	16	3	ZO
5.	Zarządzanie ryzykiem w obszarze IT	8	8	16	4	ZO
	SEMESTR II					
1.	Bezpieczeństwo informacji w usługach w chmurze	4	4	8	2	ZO
2.	Audyt systemów informatycznych	16	16	32	5	E
3.	Praktyczne aspekty audytu informatycznego	0	16	16	3	ZO
4.	Audytor systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017	4	4	8	2	ZO
5.	Komunikacja interpersonalna i zarządzanie stresem	4	4	8	1	ZO
Razem semestr I		44	44	88	17	
Razem semestr II		28	44	72	13	
RAZEM		**72**	**88**	**160**	**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. Studia dedykowane są w szczególności osobom posiadającym kwalifikacje do pełnienia funkcji Inspektorów Ochrony Danych (IOD), które chcą nabyć wiedzę i umiejętności z zakresu zarządzania bezpieczeństwem informatycznym i ryzykiem w ochronie informacji.

Absolwent Studiów Podyplomowych Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji posiada:

- wiedzę w zakresie zarządzania bezpieczeństwem informatycznym i ryzykiem w ochronie informacji;
- niezbędne przygotowanie do pracy na stanowiskach audytora systemów informatycznych oraz specjalisty ds. zarządzania ryzykiem w bezpieczeństwie informacji;
- przygotowanie uzupełniające do pracy na stanowiskach Inspektora Ochrony Danych (IOD);
- umiejętności z zakresu ochrony i bezpieczeństwa informatycznego danych w działalności instytucji publicznych i sektora prywatnego;
- umiejętności w zakresie zarządzania ryzykiem w ochronie danych osobowych oraz w obszarze IT;
- umiejętności w zakresie stosowania metod i systemów informatycznych ochrony informacji.

Absolwent studiów uzyska kwalifikacje pozwalające zajmować stanowiska pracy jako audytor systemów informatycznych oraz specjalista ds. zarządzania ryzykiem w bezpieczeństwie informacji, co będzie stanowiło dodatkowy atut w wykonywaniu zadań w przypadku osób pełniących funkcje Inspektora Ochrony Danych (IOD).

Wiedza i umiejętności będą miały charakter zarządczy, prawny i technologiczny. Dodatkowo, podczas zajęć dydaktycznych poruszane będą aspekty społeczne związane z komunikacją interpersonalną oraz stresem towarzyszącym w pracy związanej z zarządzania bezpieczeństwem informatycznym i ryzykiem w ochronie informacji.

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 ODNOSZĄCYCH 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			
MBI_W1	istotę, cele oraz normy zarządzania bezpieczeństwem informacji w organizacji	P6S_WG	P6Z_WZ, P6Z_WO
MBI_W2	zasady oraz zagrożenia i skutki wynikające z niewłaściwego przechowywania i przetwarzania danych w chmurze obliczeniowej	P6S_WG, P6S_WK	P6Z_WZ, P6Z_WO
MBI_W3	wytyczne, zasady i etapy zarządzania ryzykiem w ochronie danych osobowych i obszarze IT	P6S_WG, P6S_WK	P6Z_WT, P6Z_WZ, P6Z_WO
MBI_W4	wytyczne, zasady i etapy zarządzania incydentami i ciągłością działania w organizacji w zakresie ochrony danych osobowych i w obszarze IT	P6S_WG, P6S_WK	P6Z_WT, P6Z_WZ, P6Z_WO
MBI_W5	obszary i cele audytu informatycznego oraz metody i systemy wykorzystywane w zabezpieczaniu danych	P6S_WG, P6S_WK	P6Z_WT, P6Z_WO
MBI_W6	zasady komunikacji interpersonalnej i metody zarządzania stresem w działalności organizacji	P6S_WK	P6Z_WZ
Umiejętności: absolwent potrafi			
MBI _U1	wykorzystać wiedzę z zakresu koncepcji, metod i technik zarządzania bezpieczeństwem informatycznym w różnych sytuacjach oraz adoptować je do specyficznych warunków w zakresie ochrony informacji w organizacji	P6S_UW	P6Z_UI, P6Z_UO
MBI _U2	prowadzić audyty systemów informatycznych w organizacji	P6S_UW	P6Z_UI, P6Z_UO
MBI _U3	przeprowadzić analizę ryzyka i zagrożeń bezpieczeństwa informacji w organizacji oraz dobrać środki adekwatne do zidentyfikowanych ryzyk	P6S_UW	P6Z_UI, P6Z_UO
MBI _U4	przeprowadzić proces zarządzania incydentami wraz z prawidłowym zabezpieczeniem materiału dowodowego	P6S_UW	P6Z_UI, P6Z_UO
MBI _U5	dobrać i zastosować odpowiednie systemy informatyczne wspomagające ochronę informacji	P6S_UW	P6Z_UI, P6Z_UO, P6Z_UN

MBI _U6	prowadzić audyty systemu zarządzania bezpieczeństwem informacji	P6S_UW	P6Z_UI
MBI _U7	dobrać i zastosować metody zarządzania stresem w trudnych sytuacjach związanych z ochroną informacji w organizacji	P6S_UW	P6Z_UI, P6Z_UO
MBI _U8	komunikować się i współdziałać w grupie na potrzeby ochrony danych osobowych i w obszarze IT w organizacji	P6S_UO, P6S_UK	P6Z_UI, P6Z_UO
MBI _U9	planować własny rozwój zawodowy i podległych mu pracowników w zakresie pełnionych funkcji związanych z ochroną informacji w organizacji	P6S_UU	P6Z_UU
Kompetencje społeczne: absolwent jest gotów do			
MBI_K1	współpracy i kształtowania właściwych relacji zawodowych w organizacji	P6S_KO	P6Z_KP, P6Z_KW
MBI_K2	krytycznego oceniania posiadanej wiedzy	P6S_KK	P6Z_KP
MBI_K3	odpowiedzialnego pełnienia roli inspektora ochrony danych lub audytora, przestrzegania zasad etyki	P6S_KR, P6S_KO	P6Z_KP, P6Z_KO

MATRYCA EFEKTÓW UCZENIA SIĘ

Załącznik nr 2 do „Wytyczne do tworzenia programów studiów podyplomowych"

				Nazwa studiów podyplomowych: Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji																				
				MATRYCA POKRYCIA EFEKTÓW UCZENIA SIĘ																				
				WIEDZA							UMIEJĘTNOŚCI									KOM.SPOŁ.				
Lp.	nazwa przedmiotu	kod przedmiotu	semestr	MBI_W1	MBI_W2	MBI_W3	MBI_W4	MBI_W5	MBI_W6	kod przedmiotu	MBI_U1	MBI_U2	MBI_U3	MBI_U4	MBI_U5	MBI_U6	MBI_U7	MBI_U8	MBI_U9	MBI_K1	MBI_K2	MBI_K3	kod przedmiotu
1.	Zarządzanie ryzykiem w bezpieczeństwie informacji	SPMBI01	I	X		X				SPMBI01	X		X					X				X	SPMBI01
2.	Szacowanie ryzyka w ochronie danych osobowych	SPMBI02				X				SPMBI02			X					X					SPMBI02
3.	Systemy informatyczne wspomagające ochronę informacji	SPMBI03						X		SPMBI03	X				X								SPMBI03
4.	Zarządzanie incydentami w ochronie informacji	SPMBI04		X			X			SPMBI04				X				X				X	SPMBI04
5.	Zarządzanie ryzykiem w obszarze IT	SPMBI05		X		X				SPMBI05			X										SPMBI05
1.	Bezpieczeństwo informacji w usługach w chmurze	SPMBI06	II	X	X					SPMBI06					X			X	X				SPMBI06
2.	Audyt systemów informatycznych	SPMBI07		X			X	X		SPMBI07	X	X			X								SPMBI07
3.	Praktyczne aspekty audytu informatycznego	SPMBI08								SPMBI08	X	X			X			X					SPMBI08
4.	Audytor systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017	SPMBI09		X						SPMBI09	X					X			X		X	X	SPMBI09
5.	Komunikacja interpersonalna i zarządzanie stresem	SPMBI10							X	SPMBI10							X	X		X			SPMBI10
suma:				6	1	3	2	2	1		5	2	3	1	4	1	1	6	2	1	1	3	

RAMOWE PROGRAMY PRZEDMIOTÓW

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

<table>
<tr><td colspan="11">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td colspan="2">studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Zarządzanie ryzykiem w bezpieczeństwie informacji</td><td colspan="2">Kod przedmiotu</td><td colspan="2">SPMBI01</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td colspan="2">obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td colspan="2">Semestr</td><td colspan="2">1</td></tr>
<tr><td>8</td><td>8</td><td></td><td></td><td></td><td></td><td></td><td colspan="2">Punkty ECTS</td><td colspan="2">3</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="10">-</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="10">Celem przedmiotu jest nabycie wiedzy i kompetencji związanych z procesem oceny ryzyka i określania działań odnoszących się do ryzyk z uwzględnieniem wytycznych zawartych w normie ISO 31000:2018 oraz ISO/IEC 27005:2018.</td></tr>
<tr><td>Treści programowe</td><td colspan="10">Wykład: wymagania ISO/IEC 27001:2017 w zakresie zarządzania ryzykiem. Wytyczne w zakresie zarządzania ryzykiem wg ISO 31000:2018 i ISO/IEC 27005:2018. Zasady zarządzania ryzykiem. Pojęcia i definicje odnoszące się do zarządzania ryzykiem. Ryzyka a szanse. Kontekstowość zarządzania ryzykiem. Ćwiczenia: identyfikacja, analiza i ocena ryzyka. Metody szacowania ryzyka, w tym kryteria oceny i akceptacji ryzyka. Planowanie postępowania z ryzykiem. Deklaracja stosowania wg ISO/IEC 27001:2017 a plany postępowania z ryzykiem. Monitorowanie i przegląd ryzyka. Dokumentacja dotycząca zarządzania ryzykiem.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="10">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="10">wykład – egzamin pisemny; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="8">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="8">Słuchacz charakteryzuje istotę i zakres zarządzania ryzykiem stanowiącego kluczowe wymaganie znormalizowanego systemu zarządzania bezpieczeństwem informacji.</td><td colspan="2">MBI_W1, MBI_W3</td></tr>
<tr><td>EU2</td><td colspan="8">Słuchacz wymienia i omawia kluczowe wytyczne związane z zarządzaniem ryzykiem wg ISO 31000:2018 i ISO/IEC 27001:2017.</td><td colspan="2">MBI_W1, MBI_W3</td></tr>
<tr><td>EU3</td><td colspan="8">Słuchacz ocenia ryzyka w wybranych obszarach organizacji oraz posiada umiejętność określenia planów postępowania z ryzykiem i ich nadzorowania.</td><td colspan="2">MBI _U1, MBI _U3</td></tr>
</table>

EU4	Słuchacz komunikuje się w zakresie zagadnień dotyczących problematyki zarządzania ryzykiem w bezpieczeństwie informacji oraz współdziała w zespole z zachowaniem zasad etyki na potrzeby uruchomienia i stosowania procesu zarządzania ryzykiem.	MBI_U8, MBI_K3
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	8
	udział w ćwiczeniach	8
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	10
	samodzielne studia literatury przedmiotu	28
	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. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018. 2. PN-ISO 31000:2018 – Zarządzanie ryzykiem – Zasady i wytyczne. 3. PN-ISO 31000 – Zarządzanie ryzykiem – Zasady i wytyczne, wyd. PKN, Warszawa 2012. 4. ISO/IEC 27005:2018 - Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. 5. PN-ISO/IEC 27005:2014-01, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014.	
Literatura uzupełniająca	1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017. 2. Sitaniec I., Zawiła-Niedźwiecki J. (red.), Ryzyko operacyjne w naukach o zarządzaniu, C.H. Beck, Warszawa 2015.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	dr inż. Dariusz Kłosowski	15.01.2019

<table>
<tr><td colspan="11">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td colspan="2">studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Szacowanie ryzyka w ochronie danych osobowych</td><td colspan="2">Kod przedmiotu</td><td colspan="2">SPMBI02</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td colspan="2">obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td colspan="2">Semestr</td><td colspan="2">1</td></tr>
<tr><td>8</td><td>8</td><td></td><td></td><td></td><td></td><td></td><td colspan="2">Punkty ECTS</td><td colspan="2">3</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="10">-</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="10">Celem przedmiotu jest poznanie metod szacowania ryzyka, nabycie praktycznych umiejętności w zakresie szacowania ryzyka w ochronie danych osobowych.</td></tr>
<tr><td>Treści programowe</td><td colspan="10">Wykład: rola szacowania ryzyka w przedsiębiorstwie. Znaczenie szacowania ryzyka w realizacji obowiązków prawnych określonych w RODO. Zakres i wytyczne normy ISO27005. Charakterystyka metody CRAMM. Wytyczne Urzędu Ochrony Danych Osobowych (UODO) w zakresie szacowania ryzyka.
Ćwiczenia: identyfikacja zasobów chronionych. Podatność zasobów chronionych na ryzyka. Szacowanie ryzyka według wymagań normy ISO27005. Szacowanie ryzyka metodą CRAMM. Stosowanie w praktyce wytycznych UODO w zakresie szacowania ryzyka. Szacowanie ryzyka – podejście kompleksowe.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="10">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="10">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="8">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="8">Słuchacz wymienia i charakteryzuje metody i sposoby szacowania ryzyka.</td><td colspan="2">MBI_W3</td></tr>
<tr><td>EU2</td><td colspan="8">Słuchacz identyfikuje zasoby chronione wymagające oszacowania ryzyka.</td><td colspan="2">MBI _U3</td></tr>
<tr><td>EU3</td><td colspan="8">Słuchacz identyfikuje ryzyka i podatności dla danych osobowych.</td><td colspan="2">MBI _U3</td></tr>
<tr><td>EU4</td><td colspan="8">Słuchacz współdziałając w zespole szacuje ryzyko dla ochrony danych osobowych oraz dobiera metody minimalizacji oszacowanego ryzyka.</td><td colspan="2">MBI _U3, MBI_U8</td></tr>
</table>

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	20
	samodzielne studia literatury przedmiotu	20
	przygotowanie do zaliczenia ustnego z wykładu	18
	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	**49**	**2**

Literatura podstawowa	1. Urząd Ochrony Danych Osobowych, Poradnik RODO, Podejście oparte na ryzyku część 1. Warszawa 2018. https://uodo.gov.pl/pl/file/706 2. Urząd Ochrony Danych Osobowych, Poradnik RODO, Podejście oparte na ryzyku część 2. Warszawa 2018. https://uodo.gov.pl/pl/file/707 3. 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) 4. Wróblewski D. (red.), Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk, Narodowe Centrum Badań i Rozwoju, Józefów 2015, https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf
Literatura uzupełniająca	1. Norma PN-ISO/IEC 27005:2014-01, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014. 2. ISO/IEC 27005:2018 - Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. 3. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować wysokie ryzyko" do celów Rozporządzenia 679/2016 (WP 248).

Jednostka realizująca	Wydział Inżynierii Zarządzania PB	Data opracowania programu
Program opracował(a)	mgr Sylwia Czub-Kielczewska	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Systemy informatyczne wspomagające ochronę informacji</td><td colspan="2">Kod przedmiotu</td><td>SPMBI03</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td>Semestr</td><td>1</td></tr>
<tr><td>12</td><td>12</td><td></td><td></td><td></td><td></td><td></td><td>Punkty ECTS</td><td>4</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">-</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest dostarczenie wiedzy i umiejętności w zakresie stosowania systemów informatycznych wspomagających ochronę informacji w organizacji.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Wykład: systemy zapewniające bezpieczeństwo zasobów sieciowych. Sposoby analizy ruchu sieciowego, logów i identyfikacji zdarzeń. Metody bezpiecznego gromadzenia logów i zarządzania nimi. Rodzaje testów penetracyjnych sieci.
Ćwiczenia: systemy Firewall. Systemy wykrywania włamań - IDS (Intrusion Detection System), IPS (Intrusion Prevention System). HoneyPot. Protokoły sieciowe w analizie ruchu sieciowego - SNMP (Simple Network Management Protocol), Netflow, Sflow. Standard monitorowania sieci komputerowych - RMON (Remote Network Monitoring). Zarządzanie logami. Testy penetracyjne sieci.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="7">Słuchacz wymienia systemy informatyczne umożliwiające zapewnienie bezpieczeństwa informacji.</td><td colspan="2">MBI_W5</td></tr>
<tr><td>EU2</td><td colspan="7">Słuchacz charakteryzuje i stosuje najważniejsze systemy wykorzystywane w procesie zabezpieczeń zasobów sieciowych.</td><td colspan="2">MBI_W5, MBI _U5</td></tr>
<tr><td>EU3</td><td colspan="7">Słuchacz wymienia i charakteryzuje testy penetracyjne sieci.</td><td colspan="2">MBI_W5</td></tr>
<tr><td>EU4</td><td colspan="7">Słuchacz dobiera systemy informatyczne do określonych</td><td colspan="2">MBI_U1, MBI _U5</td></tr>
</table>

	potrzeb zabezpieczenia informacji w organizacji.	
Symbol efektu uczenia się	**Sposoby weryfikacji efektów uczenia się**	**Forma zajęć, na której zachodzi weryfikacja**
EU1	zaliczenie ustne	W
EU2	zaliczenie ustne (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C
EU3	zaliczenie ustne	W
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	24
	samodzielne studia literatury przedmiotu	31
	przygotowanie do zaliczenia ustnego z wykładu	20
	RAZEM:	**100**

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	**68**	**2,7**

Literatura podstawowa	1. Prasad P., Testy penetracyjne nowoczesnych serwisów: kompendium inżynierów bezpieczeństwa, Wydawnictwo Helion, Gliwice 2017. 2. Kim P., Podręcznik pentestera: bezpieczeństwo systemów informatycznych, Wydawnictwo Helion, Gliwice 2015. 3. Suehring S., Zapory sieciowe w systemie Linux: kompendium wiedzy o nftables, Wydawnictwo Helion, Gliwice 2015.
Literatura uzupełniająca	1. Weidman G., Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Wydawnictwo Helion, Gliwice 2015. 2. Wojciechowski P., Cisco Sourcefire: nowoczesny IPS chroniący sieć, Wydawnictwo, PRESSCOM, Wrocław 2017. 3. Thomas W., Profesjonalne testy penetracyjne. Zbuduj własne środowisko do testów, Wydawnictwo Helion, Gliwice 2014.

Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	dr inż. Paweł Tadejko	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Zarządzanie incydentami w ochronie informacji</td><td colspan="2">Kod przedmiotu</td><td>SPMBI04</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td>Semestr</td><td>1</td></tr>
<tr><td>8</td><td>8</td><td></td><td></td><td></td><td></td><td></td><td>Punkty ECTS</td><td>3</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">-</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie zarządzania incydentami w kontekście bezpieczeństwa informacji w organizacji.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Wykład: zarządzanie incydentami z zastosowaniem normy ISO/IEC 27001/2017 oraz ISO/IEC 27035/2011. Zasady planowania procesów wykrywania, raportowania, reagowania na incydenty. Doskonalenie bezpieczeństwa informacji. Ćwiczenia: pojęcie dowodu w postępowaniu. Gromadzenie elektronicznego materiału dowodowego w procesie zarządzania incydentami. Pozyskiwanie dowodów zgodnie z prawem. Przeprowadzanie dowodów i ich dopuszczenie w ramach postępowań wewnętrznych. Przygotowanie dowodów i analiz do postępowania sądowego. Autentyczność i integralność dowodów. Sporządzanie protokołów zabezpieczenia dowodów.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="7">Słuchacz opisuje zakres stosowania normy ISO/IEC 27001/2017 w kontekście zarządzania incydentami.</td><td colspan="2">MBI_W1, MBI_W4</td></tr>
<tr><td>EU2</td><td colspan="7">Słuchacz charakteryzuje zasady i etapy postępowania w zakresie zarządzania incydentami.</td><td colspan="2">MBI_W1, MBI_W4</td></tr>
<tr><td>EU3</td><td colspan="7">Słuchacz gromadzi elektroniczny materiał dowodowy w procesie zarządzania incydentem.</td><td colspan="2">MBI _U4</td></tr>
<tr><td>EU4</td><td colspan="7">Słuchacz współdziałając w zespole z zachowaniem zasad etyki zawodowej przygotowuje dowody na</td><td colspan="2">MBI _U4, MBI_U8, MBI_K3</td></tr>
</table>

	potrzeby postępowań wewnętrznych oraz sądowych.	
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	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. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018. 2. Carvey H., Altheide C., Informatyka śledcza, Przewodnik po narzędziach open source, Wydawnictwo Helion, Gliwice 2014. 3. Brzozowska M., Przygotowanie do RODO w IT, Wrocław 2018.	
Literatura uzupełniająca	1. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. 1997, nr 88, poz. 553 z późn. zm.). 2. Luttgens J., Pepe M., Mandia K., Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej, Wydawnictwo Helion, Gliwice 2016. 3. Pieleszek M., Bądź bezpieczny w cyfrowym świecie. Poradnik bezpieczeństwa IT dla każdego, Wydawnictwo Helion, Gliwice 2019.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	mgr Dariusz Gromadka	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="5">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="5"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="5" rowspan="2">Zarządzanie ryzykiem w obszarze IT</td><td colspan="2">Kod przedmiotu</td><td>SPMBI05</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td>Semestr</td><td>1</td></tr>
<tr><td>8</td><td>8</td><td></td><td></td><td></td><td></td><td></td><td>Punkty ECTS</td><td>4</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">Zarządzanie ryzykiem w bezpieczeństwie informacji</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest poznanie zasad i technik zarządzania ryzykiem w zakresie systemów informatycznych.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Wykład: modele kontroli w obszarze IT. Wytyczne audytu i kontroli systemów informatycznych pod kątem zgodności z Ustawą o ochronie danych osobowych Wprowadzenie do zarządzania ryzykiem w IT. Istota ryzyka w systemach informatycznych.
Ćwiczenia: organizacja zarządzania ryzykiem w IT. Identyfikacja ryzyka w IT. Techniki szacowania ryzyka informatycznego. Postępowanie z ryzykiem w IT. Monitorowanie poziomu ryzyka w IT. Zakres i zasady informowania o ryzyku. Risk-based audit – wykorzystanie analizy ryzyka do budowania rocznego planu audytu.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć, ocena wykonania zadania pisemnego</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="7">Słuchacz wymienia i charakteryzuje modele kontroli i istotę ryzyka w obszarze IT.</td><td colspan="2">MBI_W1, MBI_W3</td></tr>
<tr><td>EU2</td><td colspan="7">Słuchacz identyfikuje i szacuje ryzyko informatyczne.</td><td colspan="2">MBI _U3</td></tr>
<tr><td>EU3</td><td colspan="7">Słuchacz monitoruje ryzyko informatyczne.</td><td colspan="2">MBI _U3</td></tr>
<tr><td>EU4</td><td colspan="7">Słuchacz wyjaśnia zasady i na podstawie analizy ryzyka przygotowuje roczny plan audytu.</td><td colspan="2">MBI_W3, MBI _U3</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Sposoby weryfikacji efektów uczenia się</td><td colspan="2">Forma zajęć, na której zachodzi</td></tr>
</table>

		weryfikacja
EU1	zaliczenie ustne	W
EU2	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU3	ocena rozwiązania praktycznego problemu w trakcie zajęć	C
EU4	zaliczenie ustne (W), ocena wykonania zadania pisemnego (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	20
	samodzielne studia literatury przedmiotu	23
	przygotowanie do zaliczenia ustnego z wykładu	40
	RAZEM:	**100**

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	**52**	**2,1**

Literatura podstawowa	1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000). 2. Wróblewski D. (red.), Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk, Narodowe Centrum Badań i Rozwoju, Józefów 2015, https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf 3. Norma PN-ISO/IEC 27005:2014-01, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014. 4. ISO/IEC 27005:2018 - Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.
Literatura uzupełniająca	1. Urząd Ochrony Danych Osobowych, Poradnik RODO, Podejście oparte na ryzyku część 1. Warszawa 2018. https://uodo.gov.pl/pl/file/706 2. Urząd Ochrony Danych Osobowych, Poradnik RODO, Podejście oparte na ryzyku część 2. Warszawa 2018. https://uodo.gov.pl/pl/file/707 3. Kaczmarek T.T., Zarządzanie ryzykiem: ujęcie interdyscyplinarne, Difin, Warszawa 2010.

Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	inż. Artur Rudy (PIKW)	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Bezpieczeństwo informacji w usługach w chmurze</td><td colspan="2">Kod przedmiotu</td><td>SPMBI06</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td>Semestr</td><td>2</td></tr>
<tr><td>4</td><td>4</td><td></td><td></td><td></td><td></td><td></td><td>Punkty ECTS</td><td>2</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">Zarządzanie ryzykiem w bezpieczeństwie informacji</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest nabycie wiedzy i umiejętności w zakresie zarządzania bezpieczeństwem informacji oraz ochroną danych osobowych w usługach w chmurze.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Wykład: pojęcie i istota chmury obliczeniowej . Modele przetwarzania danych w chmurze. Ryzyka i szanse związane z przetwarzaniem danych w chmurze. Normy ISO/IEC 27017 i ISO/IEC 27018. Zabezpieczenia związane z przetwarzaniem danych w chmurze.
Ćwiczenia: polityka bezpieczeństwa informacji. Organizacja bezpieczeństwa informacji. Bezpieczeństwo zasobów ludzkich. Zarządzanie aktywami. Kontrola dostępu. Kryptografia. Bezpieczeństwo fizyczne i środowiskowe. Zarządzanie operacyjne. Bezpieczeństwo komunikacji. Pozyskanie systemu, rozwój i utrzymywanie. Relacje z dostawcami. Zarządzanie incydentami związanymi z bezpieczeństwem informacji. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania. Zgodność. Szkolenia.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="7">Słuchacz opisuje zakres zarządzania bezpieczeństwem informacji dotyczący usług w chmurze.</td><td colspan="2">MBI_W1, MBI_W2</td></tr>
<tr><td>EU2</td><td colspan="7">Słuchacz wymienia i charakteryzuje kluczowe wytyczne związane z zarządzaniem bezpieczeństwem informacji w usługach w chmurze wg ISO/IEC 27017 i ISO/IEC 27018.</td><td colspan="2">MBI_W2</td></tr>
<tr><td>EU3</td><td colspan="7">Słuchacz stosuje zabezpieczenia związane z przetwarzaniem danych w chmurze.</td><td colspan="2">MBI _U5</td></tr>
</table>

EU4	Słuchacz komunikuje się w zakresie zagadnień dotyczących problematyki bezpieczeństwa informacji w chmurze i planuje dalsze kierunki doskonalenia własnego i podległych pracowników w tym zakresie.	MBI_U8, MBI_U9
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	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. PN-ISO/IEC 27017:2017-07, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze. 2. PN-ISO/IEC 27018:2017-07, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII. 3. PN-ISO/IEC 27002:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji, wyd. PKN, Warszawa 2018. 4. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017.	
Literatura uzupełniająca	1. Brendan G., Wydajne systemy komputerowe: przewodnik dla administratorów systemów lokalnych i w chmurze, Wydawnictwo Helion, Gliwice 2014. 2. Krasuski A., Chmura obliczeniowa. Prawne aspekty zastosowania, WOLTERS Kluwer, Warszawa 2018. 3. Rosenberg J., Mateos A., Chmura obliczeniowa. Rozwiązania dla biznesu, Wydawnictwo Helion, Gliwice 2012.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	mgr Dariusz Gromadka	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Audyt systemów informatycznych</td><td colspan="2">Kod przedmiotu</td><td>SPMBI07</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td colspan="2">Semestr</td><td>2</td></tr>
<tr><td>16</td><td>16</td><td></td><td></td><td></td><td></td><td></td><td colspan="2">Punkty ECTS</td><td>5</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">Zarządzanie ryzykiem w bezpieczeństwie informacji, Zarządzanie ryzykiem w obszarze IT, Zarządzanie incydentami w ochronie informacji</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest zdobycie umiejętności i wiedzy niezbędnej do prowadzenia audytów systemów informatycznych.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Wykład: audyt systemów informatycznych uwagi wprowadzające: geneza, organizacje zawodowe, certyfikacja, rynek usług. Krajowe i międzynarodowe standardy audytu wewnętrznego. Znaczenie audytu IT w organizacji. Kodeks Etyki Zawodowej. Klasyfikacja audytów, Porównanie kontroli, audytu i controllingu. Procesy IT. Kontrola procesów IT. Modele dojrzałości kontroli procesów IT. Zarządzanie usługami IT. Etapy audyt procesów informatycznych. Zdarzenia, incydenty, problemy. Ciągłość działania organizacji. Odtwarzanie informacji po awarii. Krytyczność procesów i usług informatycznych. Audyt infrastruktury informatycznej.
Ćwiczenia: realizacja audytu bezpieczeństwa informacji. Polityka bezpieczeństwa i procedury. Badanie wypełniania zasad klasyfikacji informacji. Badanie świadomości roli bezpieczeństwa informacji. Audyt procesów informatycznych. Sposoby zarządzania ciągłością działania organizacji. Metody odtwarzania informacji po awarii. Analiza wpływu zdarzenia na biznes – BIA (Business Impact Analysis). Scenariusze odtwarzania obszarów. Zarządzanie projektem w realizacji biznesu. Zarządzanie zmianami. Optymalizacja wydajności procesów. Elementy zarządzania projektami zgodnie z metodologią PRINCE II. Techniki przeprowadzania audytu infrastruktury informatycznej. Identyfikacja urządzeń. Audyt procesów wspomagających realizację obszaru IT.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">wykład problemowy, ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">wykład – egzamin pisemny; ćwiczenia – ocena wykonania zadania pisemnego, ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
</table>

EU1	Słuchacz charakteryzuje istotę, cele i zasady prowadzenia audytów informatycznych.	MBI_W1, MBI_W4, MBI_W5
EU2	Słuchacz charakteryzuje poszczególne etapy prowadzenia audytu systemu informatycznego.	MBI_W5
EU3	Słuchacz wymienia, charakteryzuje i dobiera odpowiednie metody odtwarzania informacji po awarii.	MBI_W4, MBI_W5, MBI_U5
EU4	Słuchacz opracowuje plan przeprowadzenia audytu informatycznego zgodnie z metodologią PRINCE II.	MBI_U1, MBI_U2
Symbol efektu uczenia się	**Sposoby weryfikacji efektów uczenia się**	**Forma zajęć, na której zachodzi weryfikacja**
EU1	egzamin pisemny	W
EU2	egzamin pisemny	W
EU3	egzamin pisemny (W), ocena rozwiązania praktycznego problemu w trakcie zajęć (C)	W, C
EU4	ocena wykonania zadania pisemnego	C
Bilans nakładu pracy studenta (w godzinach)		**Liczba godz.**
Wyliczenie	udział w wykładach	16
	udział w ćwiczeniach	16
	udział w konsultacjach	2
	wykonanie indywidualnych zadań ćwiczeniowych	30
	samodzielne studia literatury przedmiotu	33
	przygotowanie do egzaminu pisemnego z wykładu	28
	RAZEM:	**125**
Wskaźniki ilościowe		**GODZINY** / **ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela		**34** / **1,4**
Nakład pracy studenta związany z zajęciami o charakterze praktycznym		**81** / **3,2**
Literatura podstawowa	1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017. 2. Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Wydawnictwo Helion, Gliwice 2007. 3. Norma PN-ISO/IEC 27005:2014-01, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014. 4. PN-ISO/IEC 27002:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji, wyd. PKN, Warszawa 2018. 5. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948).	
Literatura uzupełniająca	1. ISO/IEC 27005:2018 - Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. 2. Molski M., Łacheta M., Bezpieczeństwo i audyt systemów informatycznych, Wydawnictwo Uczelniane Wyższej Szkoły Gospodarki w Bydgoszczy, Bydgoszcz 2009. 3. Liderman, K., Bezpieczeństwo informacyjne, Wydawnictwo PWN, Warszawa 2012. 4. Łuczak J., Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	mgr inż. Adam Kuczyński (PIKW), mgr inż. Piotr Błaszczeć (PIKW)	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="5">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="5"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="5" rowspan="2">Praktyczne aspekty audytu informatycznego</td><td colspan="2">Kod przedmiotu</td><td>SPMBI08</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td>Semestr</td><td>2</td></tr>
<tr><td></td><td>16</td><td></td><td></td><td></td><td></td><td></td><td>Punkty ECTS</td><td>3</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">Zarządzanie ryzykiem w obszarze IT, Systemy informatyczne wspomagające ochronę informacji,</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest zdobycie umiejętności prowadzenia audytów systemów informatycznych.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Ćwiczenia: planowanie audytu informatycznego. Plan roczny i plany strategiczne. Etapy tworzenia planu audytu. Identyfikacja obszarów ryzyka. Analiza ryzyka na potrzeby planowania. Audyt poza planem. Program audytu, techniki gromadzenia dowodów i dokumentowanie wyników z audytu obszaru IT. Wywiady, listy kontrolne oraz kwestionariusze samooceny stosowane w audycie obszaru IT. Narzędzia informatyczne wykorzystywane w procesie prowadzenia audytu. Audyt infrastruktury sieciowej oraz legalności oprogramowania. Techniki przeprowadzania audytu legalności oprogramowania z wykorzystaniem dostępnych narzędzi informatycznych. Case study z zakresu audytu informatycznego w przedsiębiorstwach.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">ćwiczenia przedmiotowe, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">ćwiczenia – ocena wykonania zadania pisemnego, ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="7">Słuchacz przeprowadza, na podstawie przygotowanego planu, audyt informatyczny.</td><td colspan="2">MBI_U1, MBI_U2</td></tr>
<tr><td>EU2</td><td colspan="7">Słuchacz opracowuje dokumentację z audytu informatycznego zgodnie z obowiązującymi zasadami.</td><td colspan="2">MBI_U1, MBI_U2</td></tr>
<tr><td>EU3</td><td colspan="7">Słuchacz przeprowadza audyt legalności oprogramowania z wykorzystaniem odpowiednich</td><td colspan="2">MBI_U1, MBI_U5</td></tr>
</table>

	narzędzi informatycznych.	
EU4	Słuchacz komunikuje się i współdziała w zespole z zachowaniem zasad etyki zawodowej przy prowadzeniu audytu systemu informatycznego.	MBI_U8
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	ocena wykonania zadania pisemnego	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 ćwiczeniach	16
	udział w konsultacjach	1
	wykonanie indywidualnych zadań ćwiczeniowych	35
	samodzielne studia literatury przedmiotu	23
	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		**75** / **3**
Literatura podstawowa	1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017. 2. Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Wydawnictwo Helion, Gliwice 2007. 3. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948).	
Literatura uzupełniająca	1. Molski M., Łacheta M., Bezpieczeństwo i audyt systemów informatycznych, Wydawnictwo Uczelniane Wyższej Szkoły Gospodarki w Bydgoszczy, Bydgoszcz 2009. 2. Gałach A., Zarządzanie bezpieczeństwem systemu informatycznego – uniwersalna lista kontrolna, Wydawnictwo ODDK, Gdańsk 2005.	
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**
Program opracował(a)	mgr inż. Adam Kuczyński (PIKW), mgr inż. Piotr Błaszczeć (PIKW)	15.01.2019

<table>
<tr><td colspan="11">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="6">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td colspan="2">studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="6"></td><td colspan="2">Profil kształcenia</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="6" rowspan="2">Audytor systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2017</td><td colspan="2">Kod przedmiotu</td><td colspan="2">SPMBI09</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td colspan="2">obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td colspan="2">Semestr</td><td colspan="2">2</td></tr>
<tr><td>4</td><td>4</td><td></td><td></td><td></td><td></td><td></td><td colspan="2">Punkty ECTS</td><td colspan="2">2</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="10">Zarządzanie ryzykiem w bezpieczeństwie informacji</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="10">Celem przedmiotu jest zdobycie umiejętności i wiedzy potrzebnej do prowadzenia audytów systemu zarządzania bezpieczeństwem informacji (SZBI) ISO/IEC 27001:2017.</td></tr>
<tr><td>Treści programowe</td><td colspan="10">Wykład: rola audytora w zakresie planowania, prowadzenia raportowania oraz działań poaudytowych. Zadania audytora wiodącego a wewnętrznego. Zasady dotyczące zachowania poufności. Wymagania jednostek certyfikujących.
Ćwiczenia: ocena dokumentacji z audytów. Certyfikacja. Zasady postępowania audytora w trudnych sytuacjach. Opracowanie i realizacja audytów w organizacjach. Zakres szkoleń dla audytorów.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="10">wykład problemowy, studia przypadku, burza mózgów, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="10">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="8">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="8">Słuchacz charakteryzuje zakres normy ISO/IEC 27001:2017.</td><td colspan="2">MBI_W1</td></tr>
<tr><td>EU2</td><td colspan="8">Słuchacz ocenia dokumentację z audytów systemu zarządzania bezpieczeństwem informacji.</td><td colspan="2">MBI_U1, MBI_U6</td></tr>
<tr><td>EU3</td><td colspan="8">Słuchacz wymienia i charakteryzuje wytyczne oraz prowadzi audyty systemu zarządzania bezpieczeństwem informacji w organizacjach.</td><td colspan="2">MBI_W1, MBI_U6</td></tr>
<tr><td>EU4</td><td colspan="8">Słuchacz poprawnie dostosowuje swoje postępowanie z zachowaniem zasad etyki zawodowej w odniesieniu do trudnej sytuacji w trakcie prowadzenia audytu oraz</td><td colspan="2">MBI_K2, MBI_K3, MBI_U9</td></tr>
</table>

	krytycznie oceniając posiadaną wiedzę umiejętnie 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	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	22
	przygotowanie do zaliczenia ustnego z wykładu	8
	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		**38** / **1,5**
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)	inż. Krzysztof Smogorzewski dr inż. Dariusz Kłosowski	15.01.2019

<table>
<tr><td colspan="10">Wydział Inżynierii Zarządzania</td></tr>
<tr><td>Kierunek studiów</td><td colspan="5">Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji</td><td colspan="2">Poziom i forma studiów</td><td>studia podyplomowe</td></tr>
<tr><td>Specjalność / ścieżka dyplomowania</td><td colspan="5"></td><td colspan="2">Profil kształcenia</td><td></td></tr>
<tr><td rowspan="2">Nazwa przedmiotu</td><td colspan="5" rowspan="2">Komunikacja interpersonalna i zarządzanie stresem</td><td colspan="2">Kod przedmiotu</td><td>SPMBI10</td></tr>
<tr><td colspan="2">Rodzaj przedmiotu</td><td>obowiązkowy</td></tr>
<tr><td rowspan="2">Formy zajęć i liczba godzin</td><td>W</td><td>Ć</td><td>L</td><td>P</td><td>Ps</td><td>T</td><td>S</td><td>Semestr</td><td>2</td></tr>
<tr><td>4</td><td>4</td><td></td><td></td><td></td><td></td><td></td><td>Punkty ECTS</td><td>1</td></tr>
<tr><td>Przedmioty wprowadzające</td><td colspan="9">-</td></tr>
<tr><td>Cele przedmiotu</td><td colspan="9">Celem przedmiotu jest zapoznanie słuchaczy z zasadami komunikacji interpersonalnej oraz przyczynami i źródłami stresu, przekazanie wiedzy na temat przejawów stresu organizacyjnego, prawidłowego rozpoznawania sytuacji generujących stres i adekwatnych reakcji na jego symptomy.</td></tr>
<tr><td>Treści programowe</td><td colspan="9">Wykład: pojęcie komunikacji interpersonalnej. Pojęcie "stresu" - pozytywne i negatywne następstwa jego występowania. Źródła stresu. Stres organizacyjny.
Ćwiczenia: samoocena i jej wpływ na kształtowanie obrazu rzeczywistości. Stres wywołany niewłaściwą komunikacją interpersonalną. Rekcja na krytykę. Sposoby redukcji stresu.</td></tr>
<tr><td>Metody dydaktyczne</td><td colspan="9">wykład problemowy, studia przypadku, burza mózgów, rozwiązywanie praktycznych problemów w grupach i indywidualnie</td></tr>
<tr><td>Forma zaliczenia</td><td colspan="9">wykład – zaliczenie ustne; ćwiczenia – ocena rozwiązania praktycznego problemu w trakcie zajęć</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Zakładane efekty uczenia się</td><td colspan="2">Odniesienie do kierunkowych efektów uczenia się</td></tr>
<tr><td>EU1</td><td colspan="7">Słuchacz wymienia i charakteryzuje przyczyny i źródła stresu.</td><td colspan="2">MBI_W6</td></tr>
<tr><td>EU2</td><td colspan="7">Słuchacz wymienia i charakteryzuje zasady komunikacji interpersonalnej.</td><td colspan="2">MBI_W6</td></tr>
<tr><td>EU3</td><td colspan="7">Słuchacz analizuje sytuacje generujące stres, poprawnie dobiera sposoby zwalczania stresu.</td><td colspan="2">MBI_U7</td></tr>
<tr><td>EU4</td><td colspan="7">Słuchacz bezstresowo komunikuje się i umiejętnie utrzymuje relacje oraz w sposób prawidłowy reaguje na krytykę w trakcie współpracy w środowisku zawodowym organizacji.</td><td colspan="2">MBI_U7, MBI_U8, MBI _K1</td></tr>
<tr><td>Symbol efektu uczenia się</td><td colspan="7">Sposoby weryfikacji efektów uczenia się</td><td colspan="2">Forma zajęć, na której zachodzi</td></tr>
</table>

		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 zadań domowych	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. Cichosz A., Zarządzanie stresem w organizacji, Difin, Warszawa 2018. 2. Oppermann K., Weber E., Style porozumiewania w pracy, GWP, Gdańsk, 2007. 3. Goleman D., Inteligencja emocjonalna w praktyce, "Media Rodzina" Poznań, 2009.		
Literatura uzupełniająca	1. Zawadzka A. (red.), Psychologia zarządzania w organizacji, PWN, Warszawa 2010. 2. Adler R.B., Rosenfeld L.B., Russell F., Relacje interpersonalne. Proces porozumiewania się, Dom Wydawniczy REBIS, Poznań 2016.		
Jednostka realizująca	Wydział Inżynierii Zarządzania PB	**Data opracowania programu**	
Program opracował(a)	dr Joanna Szydło	15.01.2019	

ZASOBY BIBLIOTECZNE ORAZ ELEKTRONICZNE ZASOBY WIEDZY OBEJMUJĄCE LITERATURĘ ZALECANĄ NA STUDIACH PODYPLOMOWYCH MENEDŻER DS. BEZPIECZEŃSTWA INFORMATYCZNEGO I RYZYKA W OCHRONIE INFORMACJI, DO KTÓRYCH UCZELNIA ZAPEWNIA DOSTĘP

Biblioteka Politechniki Białostockiej zapewnia dostęp do zasobów bibliotecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną na Studiach Podyplomowych Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji.

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 akademiccy 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 nauczycieli akademickich 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
1.	Łącznie zasoby (liczba woluminów), w tym:	406 331
	wydawnictwa zwarte	281 495
	wydawnictwa ciągłe	45 907
	zbiory specjalne (normy, literatura firmowa, dokumenty elektroniczne)	78 929
2.	Liczba czasopism prenumerowanych (dostępnych w formie papierowej), w tym:	419
	wydawnictwa polskie	389
	wydawnictwa zagraniczne	30
3.	Liczba wydawnictw zarejestrowanych (liczba woluminów), w tym:	6 821
	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 wypożyczania 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 czytelni 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 wielodziedzinowe 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 Managament 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 wchodzą 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 pozycji 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 (regały 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 regały);
- wolny dostęp do wszystkich bieżących (5 regałów) i niektórych archiwalnych numerów czasopism i gazet (8 regałów);
- 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 akademiccy 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 bibliotecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną na Studiach Podyplomowych Menedżer ds. bezpieczeństwa informatycznego i ryzyka w ochronie informacji:

zasoby biblioteczne:

1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowe PWN, Warszawa 2017.
2. Brendan G., Wydajne systemy komputerowe: przewodnik dla administratorów systemów lokalnych i w chmurze, Helion, Gliwice 2014.
3. Brzozowska M., Przygotowanie do RODO w IT, Wrocław 2018.
4. Carvey H., Altheide C., Informatyka śledcza, Przewodnik po narzędziach open source, Wydawnictwo Helion, Gliwice 2014.
5. Carvey, H., Analiza śledcza i powłamaniowa: zaawansowane techniki prowadzenia analizy w systemie Windows 7, Wydawnictwo Helion, Gliwice 2013.
6. Cichosz A., Zarządzanie stresem w organizacji, Difin, Warszawa 2018.
7. Goleman D., Inteligencja emocjonalna w praktyce, "Media Rodzina" Poznań, 2009.
8. Kaczmarek T.T., Zarządzanie ryzykiem: ujęcie interdyscyplinarne, Difin, Warszawa 2010.
9. Kim P., Podręcznik pentestera: bezpieczeństwo systemów informatycznych, Wydawnictwo Helion, Gliwice 2015.

10. Molski M., Łacheta M., Przewodnik audytora systemów informatycznych, Wydawnictwo Helion, Gliwice 2007.
11. Oppermann K., Weber E., Style porozumiewania w pracy, GWP, Gdańsk, 2007.
12. PN-ISO 31000 – Zarządzanie ryzykiem – Zasady i wytyczne, wyd. PKN, Warszawa 2012.
13. PN-ISO/IEC 27001:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania, wyd. PKN, Warszawa 2018.
14. PN-ISO/IEC 27002:2017-06, Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji, wyd. PKN, Warszawa 2018.
15. PN-ISO/IEC 27005:2014-01, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem
w bezpieczeństwie informacji, wyd. PKN, Warszawa 2014.
16. Prasad P., Testy penetracyjne nowoczesnych serwisów: kompendium inżynierów bezpieczeństwa, Wydawnictwo Helion, Gliwice 2017.
17. Sitaniec I., Zawiła-Niedźwiecki J. (red.), Ryzyko operacyjne w naukach o zarządzaniu, C.H. Beck, Warszawa 2015.
18. Suehring S., Zapory sieciowe w systemie Linux: kompendium wiedzy o nftables, Wydawnictwo Helion, Gliwice 2015.
19. Wojciechowski P., Cisco Sourcefire: nowoczesny IPS chroniący sieć, Wydawnictwo, PRESSCOM, Wrocław 2017.
20. Zawadzka A. (red.), Psychologia zarządzania w organizacji, PWN, Warszawa 2010.

elektroniczne zasoby wiedzy:

1. Łukacz J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Poznań 2009, https://jacekluczak.pl/images/download/Systemowe.pdf
2. Poradnik GIODO: Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych, Warszawa 2016, https://www.giodo.gov.pl/pl/1520074/9761
3. 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)
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. Strona internetowa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl
6. Urząd Ochrony Danych Osobowych, Poradnik RODO, Podejście oparte na ryzyku część 1. Warszawa 2018. https://uodo.gov.pl/pl/file/706
7. Urząd Ochrony Danych Osobowych, Poradnik RODO, Podejście oparte na ryzyku część 2. Warszawa 2018. https://uodo.gov.pl/pl/file/707
8. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
9. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. 1997, nr 88, poz. 553 z późn. zm.).
10. Wróblewski D. (red.), Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk, Narodowe Centrum Badań i Rozwoju, Józefów 2015, https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf

11. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować wysokie ryzyko" do celów Rozporządzenia 679/2016 (WP 248)

zasoby biblioteczne przeznaczone do zakupienia po ukazaniu się ich polskojęzycznych wersji:

1. PN-ISO/IEC 27017:2017-07, Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze.
2. PN-ISO/IEC 27018:2017-07, Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII

OPINIA WYDZIAŁOWEJ KOMISJI DS. JAKOŚCI KSZTAŁCENIA WYDZIAŁU INŻYNIERII ZARZĄDZANIA DOTYCZĄCA PROGRAMU STUDIÓW PODYPLOMOWYCH MENEDŻER DS. BEZPIECZEŃSTWA INFORMATYCZNEGO I RYZYKA W OCHRONIE INFORMACJI

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 „Menedżer ds. Bezpieczeństwa Informatycznego i Ryzyka w Ochronie Informacji".

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 „Menedżer ds. Bezpieczeństwa Informatycznego i Ryzyka w Ochronie Informacji" jest bardzo aktualny i pozwoli słuchaczom na uzyskanie niezbędnej w tym kierunku wiedzy, umiejętności i kompetencji. Postanowiono pozytywnie program zaopiniować.

Przewodniczący WK ds. JK
dr inż. Arkadiusz Łukjaniuk

UCHWAŁA NR 10/2/2019 RADY WYDZIAŁU INŻYNIERII ZARZĄDZANIA Z DNIA 06.02.2019 R. W SPRAWIE URUCHOMIENIA STUDIÓW PODYPLOMOWYCH: MENEDŻER DS. BEZPIECZEŃSTWA INFORMATYCZNEGO I RYZYKA W OCHRONIE INFORMACJI - I EDYCJA I POWOŁANIA KIEROWNIKA TYCH STUDIÓW

Uchwała nr 10/2/2019
Rady Wydziału Inżynierii Zarządzania

z dnia 6 lutego 2019 roku

w sprawie uruchomienia studiów podyplomowych: Menedżer ds. Bezpieczeństwa Informatycznego i Ryzyka w Ochronie Informacji I 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: **Menedżer ds. Bezpieczeństwa Informatycznego i Ryzyka w Ochronie Informacji I 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. Jagmin Ejdys, prof. nzw.