Załącznik nr 9

do protokołu z posiedzenia Rady Wydziału Ekonomii i Zarządzania

Uniwersytetu w Białymstoku z dnia 04.09.2017r.

UCHWAŁA Nr 427/X/17

Rady Wydziału Ekonomii i Zarządzania Uniwersytetu w Białymstoku

z dnia 4 września 2017 r.

w sprawie planu studiów, programu i efektów

kształcenia Studiów Podyplomowych

Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym

od cyklu kształcenia 2017/2018

Działając na podstawie Uchwały Nr 2081 Senatu Uniwersytetu w Białymstoku z dn. 31.05.2017 r. w sprawie wytycznych dla rad podstawowych jednostek organizacyjnych Uniwersytetu, określających zasady tworzenia planów i programów studiów podyplomowych oraz kursów dokształcających i szkoleń.

§ 1

Uchwala plan, program oraz efekty kształcenia Studiów Podyplomowych Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym od cyklu kształcenia 2017/2018

§ 2

Wyniki głosowania:

Uprawnionych do głosowania: 46; Osób obecnych : 32

Głosów oddanych: 27; ważnych: 27; nieważnych: 0
Za: 27
Przeciw: 0
Wstrzymujących: 0

§ 3

Uchwała wchodzi w życie z dniem jej podpisania.

Przewodniczący
Rady Wydziału Ekonomii i Zarządzania
Uniwersytetu w Białymstoku

Dr hab. Marzanna Poniatowicz, prof. UwB

Załącznik nr 1
do Uchwały nr 2081
Senatu Uniwersytetu w Białymstoku
z dnia 31 maja 2017 roku

EFEKTY KSZTAŁCENIA

studiów podyplomowych „Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym"

1. Jednostka prowadząca studia podyplomowe: **Uniwersytet w Białymstoku, Wydział Ekonomii i Zarządzania, Zakład Ekonomiki i Finansów Samorządu Terytorialnego**

2. Kwalifikacje nadawane po ukończeniu studiów podyplomowych na poziomie: **Ukończenie podyplomowych studiów „Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym" pozwoli absolwentowi nabyć szeroki zakres specjalistycznej wiedzy teoretycznej i praktycznych umiejętności z zakresu zarządzania bezpieczeństwem informacji niezbędnych do efektywnego, zgodnego z prawem, sprawnego i profesjonalnego wykonywania zadań administratora bezpieczeństwa informacji (od maja 2018 roku inspektora ochrony danych) oraz zadań administratora danych osobowych i procesora. Ukończenie studiów podyplomowych „Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym" będzie stanowiło podstawę do wykazania spełnienia przewidzianych w przepisach prawa wymogów stawianych zarówno obecnemu administratorowi bezpieczeństwa informacji, jak i inspektorowi ochrony danych po dniu 25 maja 2018 roku.**

3. Umiejscowienie studiów w obszarze/obszarach kształcenia *(z uwzględnieniem dziedziny/dziedzin nauki)*: **nauki społeczne (ekonomia, zarządzanie, prawo)**

4. Ogólne cele kształcenia: **Głównym celem studiów jest przekazanie specjalistycznej wiedzy teoretycznej i praktycznych umiejętności z zakresu zarządzania bezpieczeństwem informacji niezbędnych do efektywnego, zgodnego z prawem, sprawnego i profesjonalnego wykonywania zadań administratora bezpieczeństwa informacji (od maja 2018 roku inspektora ochrony danych) oraz zadań administratora danych osobowych i procesora. Zdobyte w czasie studiów kwalifikacje zawodowe pozwolą absolwentom profesjonalnie wykonywać i organizować własną pracę, ale też przygotować się do wykonywania zadań na stanowisku administratora bezpieczeństwa informacji w danym podmiocie sektora publicznego, skutecznie zbudować efektywną współpracę administratora bezpieczeństwa informacji z administratorem danych lub procesorem, profesjonalnie szkolić personel, po to by spełniać wymogi określone przepisami prawa, usprawniać działanie organizacji i zapewniać ochronę danych osobowych zarówno personelu wewnętrznego, jak i osób obsługiwanych przez dany podmiot.**

5. Wskazanie, czy w procesie definiowania efektów kształcenia uwzględniono zapotrzebowanie otoczenia społeczno-gospodarczego: **W procesie definiowania efektów kształcenia uwzględniono potrzeby organizacji (jednostki sektora publicznego) w zakresie podnoszenia efektywności i spełniania przez organizację obowiązków nakładanych przez przepisy prawa, jak również wyzwania dla organizacji związanych z pozyskaniem i utrzymaniem kompetentnych osób posiadających specjalistyczną wiedzę i kompetencje niezbędne do pełnienia zadań administratora bezpieczeństwa informacji oraz inspektora danych osobowych. Uwzględnione zostały również potrzeby administratorów danych osobowych oraz procesorów sektora publicznego.**

6. Wymagania wstępne *(oczekiwane kompetencje kandydata)*: **Kandydat na studia podyplomowe jest absolwentem studiów I bądź II stopnia (licencjackich lub magisterskich) i dostrzega potrzebę nabycia lub poszerzenia kompetencji zawodowych w zakresie zarządzania bezpieczeństwem informacji w organizacji.**

Symbol* opisu charakterystyk II stopnia PRK	OPIS CHARAKTERYSTYK II STOPNIA PRK	Symbol** efektu kształcenia	OPIS ZAKŁADANYCH EFEKTÓW KSZTAŁCENIA Po ukończeniu studiów podyplomowych absolwent:
WIEDZA, absolwent zna i rozumie:			
S_P7S _WG	W pogłębionym stopniu – wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące: ▪ zaawansowaną wiedzę ogólną z zakresu dyscyplin naukowych lub artystycznych tworzących podstawy teoretyczne, ▪ uporządkowaną i podbudowaną teoretycznie wiedzę obejmującą kluczowe zagadnienia ▪ wybrane zagadnienia z zakresu wiedzy szczegółowej właściwe dla programu kształcenia	S_P7S _WG01	Zna zakres zadań i kompetencji administratora bezpieczeństwa informacji, administratora danych osobowych oraz procesora.
		S_P7S _WG02	Zna i rozumie modelowy system zarządzania bezpieczeństwem informacji w organizacji.
		S_P7S _WG03	Zna narzędzia i metody wykonywania zadań administratora bezpieczeństwa informacji oraz administratora danych osobowych.
		S_P7S _WG04	Zna obowiązujące regulacje prawne z zakresu ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznych oraz regulacje wynikające z reformy w 2018 roku.
		S_P7S _WG05	Zna i rozumie podstawy zarządzania wiedzą, ciągłością działania, ryzykiem, incydentami w organizacji.
		S_P7S _WG06	Zna i rozumie pojęcie audytu bezpieczeństwa informacji, etapy i zasady jego planowania i realizacji.
		S_P7S _WG07	Zna i rozumie zakres stosowania normy ISO 27001.
		S_P7S _WG08	Ma elementarną wiedzę na temat ryzyk w organizacji i analizy ryzyka.
		S_P7S _WG09	Ma wiedzę na temat prowadzenia szkoleń wewnętrznych dla osób przetwarzających dane osobowe.
		S_P7S _WG10	Rozumie potrzebę tworzenia, weryfikacji i aktualizacji dokumentacji związanej z ochroną danych osobowych w jednostkach sektora publicznego.
		S_P7S _WG11	Ma podstawową wiedzę w zakresie regulacji odnoszących się do informacji niejawnych.
		S_P7S _WG12	Ma wiedzę dotyczącą zasad udostępniania informacji publicznej.
		S_P7S _WG13	Ma wiedzę na temat kierunków rozwoju e-usług w

			jednostkach sektora publicznego.
S_P7S _WK	Zna i rozumie ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z nadaną kwalifikacją, w tym zasad ochrony własności przemysłowej i prawa autorskiego	S_P7S _WK01	Zna i rozumie podstawową terminologię nauk o zarządzaniu, ekonomiczną, prawniczą i informatyczną dotyczącą obszaru ochrony danych osobowych w jednostce sektora publicznego.
		S_P7S_WK02	Zna i rozumie podstawy m.in. prawne i finansowe funkcjonowania jednostek sektora publicznego oraz podstawy zarządzania w tych jednostkach.
		S_P7S_WK03	Zna procesy zachodzące w organizacji wymagające zaangażowania administratora bezpieczeństwa informacji.
		S_P7S_WK04	Posiada niezbędną wiedzę w zakresie funkcjonowania systemów informatycznych i nowoczesnych technologii stosowanych w jednostkach administracji publicznej.
		S_P7S_WK05	Rozumie rolę komunikacji w organizacji i proces przepływu informacji.
		S_P7S_WK06	Rozumie istotę oddziaływania kultury organizacyjnej i instrumentów z nią związanych na sprawność i skuteczność zarządzania bezpieczeństwem informacji.
		S_P7S_WK07	Rozumie istotę zachowań etycznych i nieetycznych.
		S_P7S_WK08	Rozumie wpływ nowoczesnych technologii na ochronę danych osobowych.
UMIEJĘTNOŚCI, absolwent potrafi:			
S_P7S _UW	Potrafi wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez: ▪ właściwy dobór źródeł oraz informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy, syntezy oraz twórczej interpretacji i prezentacji tych informacji ▪	S_P7S_UW01	Potrafi reagować na incydenty naruszenia procedur związanych z ochroną danych osobowych w organizacji.
		S_P7S_UW02	Posiada umiejętność interpretowania i odpowiedniego stosowania przepisów prawa z dziedziny ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej.
		S_P7S_UW03	Potrafi nadzorować, tworzyć i gromadzić dokumentację z zakresu ochrony danych osobowych wymaganą przepisami prawa.
		S_P7S_UW04	Potrafi stosować najistotniejsze zapisy normy ISO 27001

	dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych (ICT)	S_P7S_UW05	Potrafi szacować i analizować ryzyka dla systemu bezpieczeństwa informacji, wskazywać możliwości przeciwdziałania im oraz obniżać ich poziom.
		S_P7S_UW06	Potrafi korzystać z e-usług.
		S_P7S_UW07	Potrafi nadzorować procesy mające związek z ochroną danych osobowych.
S_P7S _UK	Potrafi komunikować się na tematy specjalistyczne ze specjalistycznym kręgiem odbiorców, prowadzić debatę, posługiwać się językiem obcym na poziomie B2+	S_P7S_UK01	Potrafi, planować, przeprowadzać i analizować rozmowy z administratorem danych osobowych oraz procesorem i właścicielami zasobów informacyjnych.
		S_P7S_UK02	Potrafi opracować rekomendacje dla organizacji mające na celu podniesienie poziomu zarządzania bezpieczeństwem informacji.
		S_P7S_UK03	Potrafi rozróżnić etyczne i nieetyczne zachowania w stosunkach w organizacji mające związek z ochroną danych osobowych i znaleźć sposoby przeciwdziałania nim.
S_P7S _UO	Potrafi kierować pracą zespołu	S_P7S_UO01	Posiada umiejętność pracy analitycznej i koncepcyjnej.
		S_P7S_UO02	Potrafi zaplanować własne działania w celu wykonania obowiązków administratora bezpieczeństwa informacji.
		S_P7S_UO03	Potrafi wskazać korzyści ze stosowania nowoczesnych technologii w organizacji.
		S_P7S_UO04	Potrafi rozpoznawać zagrożenia wynikające z nowoczesnych technologii i błędu ludzkiego.
S_P7S _UU	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie	S_P7S_UU01	Potrafi prowadzić szkolenia wewnętrzne dla personelu z zakresu ochrony danych osobowych.
		S_P7S_UU02	Potrafi skutecznie motywować siebie i innych do zdobywania wiedzy.
		S_P7S_UU03	Potrafi rozpoznawać style efektywnego uczenia się, aby poprawiać efektywność wykonywanej pracy.
KOMPETENCJE SPOŁECZNE, absolwent jest gotów do:			
S_P7S _KK	Jest gotów do krytycznej oceny odbieranych treści, uznawania znaczenia wiedzy w	S_P7S_KK01	Doskonali zdolność pokonywania problemów i trudności wynikających z kontaktów

	rozwiązywaniu problemów poznawczych i praktycznych		interpersonalnych i hierarchii w organizacji.
		S_P7S_KK02	Ma świadomość własnego wpływu na organizację poprzez kształtowanie i poprawę funkcjonalności systemu zarządzania bezpieczeństwem informacji.
S_P7S _KO	Jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, inicjowania działania na rzecz interesu publicznego, myślenia i działania w sposób przedsiębiorczy	S_P7S_KO01	Ma świadomość potrzeby samodoskonalenia, podnoszenia własnych kompetencji ważnych w relacjach interpersonalnych i funkcjonowaniu organizacji.
		S_P7S_KO02	Ma świadomość potrzeby skutecznego motywowania współpracowników, podwładnych.
S_P7S _KR	Jest gotów do odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych, w tym: ▪ rozwijania dorobku zawodu, ▪ podtrzymywania etosu zawodu, ▪ przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad	S_P7S_KR01	Podnosi poziom umiejętności budowania relacji interpersonalnych.
		S_P7S_KR02	Podnosi poziom umiejętności wystąpień publicznych w zakresie prowadzenia szkoleń.
		S_P7S_KR03	Potrafi inspirować i organizować proces uczenia się innych osób.
		S_P7S_KR04	Potrafi pracować w zespole, przyjmując w nim różne role.
		S_P7S_KR05	Doskonali skuteczne metody komunikacji i negocjacji w wykonywaniu zadań administratora bezpieczeństwa informacji, administratora danych osobowych, procesora.

DZIEKAN
WYDZIAŁU EKONOMII I ZARZĄDZANIA
dr hab. Marzanna Poniatowicz
prof. UwB

.....
(pieczątka i podpis dziekana)

Objaśnienia oznaczeń:

** S_P7S_WG – przykładowy symbol opisu charakterystyk II stopnia PRK*

S *- obszar kształcenia w zakresie nauk społecznych* ***H*** *- obszar kształcenia w zakresie nauk humanistycznych* ***P*** *- obszar kształcenia w zakresie nauk przyrodniczych* ***X*** *- obszar kształcenia w zakresie nauk ścisłych* *T - obszar kształcenia w zakresie nauk technicznych*
P6 lub **P7** – poziom PRK **S** – charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa

*** SP7_WG01– przykładowy symbol efektu kształcenia*

SP7 *efekty kształcenia dla studiów podyplomowych na poziomie 6 lub 7 PRK*

wyższego
W – wiedza *(kategoria opisowa)*
G – *głębia i zakres*
K - *kontekst*
U – umiejętności *(kategoria opisowa)*
W – *wykorzystanie wiedzy*
K – *komunikowanie się*
O – *organizacja pracy*
U – *uczenie się*
K – kompetencje społeczne *(kategoria opisowa)*
K – *krytyczna ocena*
O - *odpowiedzialność*
R – *rola zawodowa*

W – wiedza *(kategoria opisowa)*
G – *głębia i zakres*
K - *kontekst*
U – umiejętności *(kategoria opisowa)*
W – *wykorzystanie wiedzy*
K – *komunikowanie się*
O – *organizacja pracy*
U – *uczenie się*
K – kompetencje społeczne *(kategoria opisowa)*
K – *krytyczna ocena*
O - *odpowiedzialność*
R – *rola zawodowa*
01, 02, 03 i kolejne – *numer efektu kształcenia*

Załącznik nr 2
do Uchwały nr 2081
Senatu
Uniwersytetu w Białymstoku
z dnia 31 maja 2017 r.

PROGRAM STUDIÓW PODYPLOMOWYCH

I. INFORMACJE OGÓLNE

1. Nazwa jednostki prowadzącej studia podyplomowe:

   Uniwersytet w Białymstoku, Wydział Ekonomii i Zarządzania, Zakład Ekonomiki i Finansów Samorządu Terytorialnego

2. Nazwa studiów podyplomowych:

   Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym

3. Czas trwania studiów podyplomowych:

   2 semestry

4. Założenia ogólne:

   Założeniem studiów podyplomowych „Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym" jest wyposażenie absolwenta w ustrukturyzowaną oraz aktualną wiedzę, a także praktyczne umiejętności z obszarów związanych ze specyfiką zadań wykonywanych przez administratorów bezpieczeństwa informacji, administratorów danych osobowych, procesorów.

5. Ogólna liczba punktów ECTS konieczna do uzyskania kwalifikacji podyplomowych:

   60 punktów

6. Ogólna liczba godzin zajęć dydaktycznych:

   170 godzin

7. Program uchwalony na posiedzeniu Rady Wydziału w dniu ***4 września 2017 roku*** obowiązuje od ***roku akademickiego 2017/2018***.

II. WYKAZ PRZEDMIOTÓW

Przedmioty	Punkty ECTS	Odniesienie do zakładanych efektów kształcenia	Sposób weryfikacji zakładanych efektów kształcenia
WYKŁAD WPROWADZAJĄCY, 2 godz.			
MODUŁ I: Obszar ekonomiczny w bezpieczeństwie informacji 32 godziny, 12 punktów ECTS			
1) Podstawy zarządzania w kontekście	1,5	S_P7S _WK01, S_P7S _WG02, SP7_WK03, S_P7S _WG05, S_P7S_WK06, S_P7S_UW07,	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach

bezpieczeństwa informacji		S_P7S_KK02	poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
2) Stosowanie Normy ISO 27001 w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)	3	S_P7S_WK03, S_P7S _WG07, S_P7S_WK04, S_P7S_UW04, S_P7S_KK02, S_P7S_KR04	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
3) Audyt SZBI	3	S_P7S _WG02, S_P7S_WK03, S_P7S _WG06, S_P7S_UK02, S_P7S_UK01, S_P7S_UW07, S_P7S_KK01, S_P7S_KR04	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
4) Planowanie ciągłości działania	1,5	S_P7S _WG05, S_P7S _WG10, S_P7S_UO01, S_P7S_UW01, S_P7S_UW07, S_P7S_KK01, S_P7S_KK02	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
5) Zarządzanie ryzykiem	1,5	SP7_WK03, S_P7S _WG05, S_P7S _WG08, S_P7S_UW05, S_P7S_UO04, S_P7S_KK01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
6) Zarządzanie incydentami	1,5	S_P7S_UW01, S_P7S_UW03, S_P7S _WG05, S_P7S_UO04, S_P7S_KK01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
MODUŁ II: Regulacje międzynarodowe, unijne i krajowe w obszarze bezpieczeństwa informacji 50 godzin, 19 punktów ECTS			

1) Ustrój administracji rządowej i samorządowej oraz specyfika jednostek sektora publicznego	3	S_P7S _WK01, S_P7S_WK02, S_P7S_KK01, S_P7S_KK02, S_P7S_WK03	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
2) Normy prawa i dobre praktyki w ochronie informacji i danych osobowych	3	S_P7S _WK01, S_P7S _WG04, S_P7S _WG01, S_P7S _WG03, S_P7S _WG10, S_P7S _WG11, S_P7S_UW02, S_P7S_UW03, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
3) Pakiet reformujący ochronę danych osobowych	3	S_P7S _WG01, S_P7S _WG04, S_P7S _WK01, S_P7S _WG03, S_P7S_WK06, S_P7S_UW02, S_P7S_UW03, S_P7S_UO01, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
4) Status prawny administratorów bezpieczeństwa informacji/inspektoró w ochrony danych, administratorów danych osobowych i procesorów	3	S_P7S _WG01, S_P7S _WG02, S_P7S _WG03, SP_ S_P7S _WG10, S_P7S_WK03, S_P7S_UW03, S_P7S_UO01, S_P7S_UO02, S_P7S_UK01, S_P7S_KK02, S_P7S_KR01, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
5) Organy ochrony danych osobowych	1,5	S_P7S _WG04, S_P7S _WG10, S_P7S_UW02, S_P7S_UW03, S_P7S_KO02	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
6) Informacje niejawne (zagadnienia ogólne i	1,5	S_P7S _WG11, S_P7S _WG04, S_P7S_UW02,	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne)

rozwiązania praktyczne)		S_P7S_UO01, S_P7S_KO01, S_P7S_KR05	poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
7) Dostęp do informacji publicznej (zagadnienia ogólne i rozwiązania praktyczne)	3	S_P7S _WK01, S_P7S _WG11, S_P7S _WG12, S_P7S_UW02, S_P7S_UO01, S_P7S_KO01, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
8) Odpowiedzialność w obszarze ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej	1	S_P7S _WK01, S_P7S _WG11, S_P7S_UW02, S_P7S_UO01, S_P7S_KK02, S_P7S_UK03, S_P7S_KO01, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
MODUŁ III: Standardy zarządzania bezpieczeństwem informacji: studium przypadków – rozwiązania praktyczne 24 godziny, 8 punktów ECTS			
1) Realizacja zadań z zakresu ochrony danych osobowych w oparciu o zasoby własne lub outsourcing	1	S_P7S _WG01, S_P7S _WG02, S_P7S _WG03, S_P7S _WG04, S_P7S_WK03, S_P7S_WK06, S_P7S_UW03, S_P7S_UK02, S_P7S_UO02, s_P7S_UW07, S_P7S_UK03, S_P7S_UK01, S_P7S_KK02, S_P7S_KR04	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
2) Aspekty praktyczne w SZBI	4	S_P7S _WG02, S_P7S _WG03, S_P7S_WK03, S_P7S_WK04, S_P7S_WK06, S_P7S_WK05, S_P7S_UW03, S_P7S_UK02, S_P7S_UW07,	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego

		S_P7S_KK01, S_P7S_KR04	(obrona pracy).
3) Powierzenie danych osobowych do przetwarzania podmiotom trzecim	1,5	S_P7S _WG04, S_P7S _WK01, SP7_WK02, S_P7S_WK03, S_P7S _WG03, S_P7S_UW02, S_P7S_UW03, S_P7S_UO01, S_P7S_UW07, S_P7S_KK02, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
4) Dobre praktyki w SZBI	1,5	S_P7S _WG03, S_P7S _WG02, S_P7S_WK03, S_P7S_WK04, S_P7S_WK05, S_P7S_WK06, S_P7S_UW03, S_P7S_UW07, S_P7S_UK02, S_P7S_KK01, S_P7S_KR04	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
MODUŁ IV: Kompetencje miękkie w bezpieczeństwie informacji 22 godziny, 8 punktów ECTS			
1) Czynnik ludzki w bezpieczeństwie informacji	1,5	S_P7S_WK05, S_P7S_UU01, S_P7S _WG05, S_P7S_WK06, S_P7_WK07, SP_7S_UK01, S_P7S_UK03, S_P7S_UO04, S_P7S_KK01, S_P7S_KO02, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
2) Wymiana informacji, dzielenie się wiedzą, samodoskonalenie się	1,5	S_P7S _WG03, S_P7S _WG05, SP7_WK05, S_P7S _WG09, S_P7S_UK03, S_P7S_UO01, S_P7S_UU01, S_P7S_UU03, S_P7S_KR01, S_P7S_KR03, S_P7S_KO01, S_P7S_KO02, S_P7S_KR04	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).

3) Wystąpienia publiczne, w tym narzędzia budowania efektownych prezentacji	3	S_P7S _WG03, S_P7S _WG09, S_P7S_UU01, S_P7S_UU02, S_P7S_UU03, S_P7S_KO02, S_P7S_KR02, S_P7S_KR03	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
4) Komunikacja a bezpieczeństwo informacji	1	S_P7S_WK03, S_P7S_WK05, S_P7S_WK06, S_P7S_UW07, S_P7S_UK01, S_P7S_UK03, S_P7S_KK01, S_P7S_KK02, S_P7S_KR01, S_P7S_KR04, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
5) Etyka zawodowa w bezpieczeństwie informacji	1	S_P7S_UK03, S_P7S_WK07, S_P7S_KK01, S_P7S_KR05	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
MODUŁ V: Rozwiązania techniczno-informatyczne w bezpieczeństwie informacji 28 godzin, 10 punktów ECTS			
1) Aspekty techniczne w bezpieczeństwie informacji	3	S_P7S _WG02, S_P7S _WG03, S_P7S_WK03, S_P7S_WK04, S_P7S_WK05, S_P7S_WK08, S_P7S_UW07, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
2) Cloud computing w bezpieczeństwie informacji	1	S_P7S_WK04, S_P7S_WK08, S_P7S _WG03, S_P7S_UO03, S_P7S_UO04, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego

			(obrona pracy).
3) Bezpieczeństwo infrastruktury informatycznej	1	S_P7S _WG02, S_P7S _WG03, S_P7S_WK03, S_P7S_WK04, S_P7S_WK08, S_P7S_UO03, S_P7S_UO04, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
4) Kryptografia i inne mechanizmy bezpieczeństwa	1	S_P7S _WG03, S_P7S _WG02, S_P7S_WK03, S_P7S_WK04, S_P7S_WK08, S_P7S_UO03, S_P7S_UO04, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
5) Cyberterroryzm	1	S_P7S _WG02, S_P7S _WG03, S_P7S_WK03, S_P7S_WK04, S_P7S_WK08, S_P7S_UO03, S_P7S_UO04, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
6) Nowoczesne technologie a ochrona danych osobowych	1	S_P7S _WG02, S_P7S _WG03, S_P7S_WK03, S_P7S_WK04, S_P7S_WK08, S_P7S_UO03, S_P7S_UO04, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).
7) Sfera publicznych e-usług	2	S_P7S _WG03, S_P7S_WK03, S_P7S_WK04, S_P7S _WG13, S_P7S_WK08, S_P7S_UO03, S_P7S_UO02, S_P7S_UW06, S_P7S_KO01	Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. obecność, test, projekt, referat itp.); poprzez seminarium dyplomowe i przygotowanie pracy dyplomowej, a także w trakcie egzaminu dyplomowego (obrona pracy).

Seminarium dyplomowe 10 godzin, 3 punkty ECTS
WYKŁAD KOŃCZĄCY, 2 godz.

III. ZASADY, FORMY I WYMIAR ODBYWANIA PRAKTYK ZAWODOWYCH wraz z przyporządkowaną im liczbą punktów ECTS *(jeżeli program studiów podyplomowych przewiduje realizację praktyk)*

Nie dotyczy.

IV. WARUNKI UKOŃCZENIA STUDIÓW PODYPLOMOWYCH

Uzyskanie zaliczeń z pięciu modułów (na podstawie obecności w zajęciach poszczególnych przedmiotów bądź w formie ustalonej z prowadzącymi zajęcia);

Obrona pracy dyplomowej (na ostatnim zjeździe).

DZIEKAN
WYDZIAŁU EKONOMII I ZARZĄDZANIA
dr hab. Marzanna Poniatowicz
prof. UwB

.....

(pieczątka i podpis dziekana)

UNIWERSYTET W BIAŁYMSTOKU

Załącznik nr 3
do Uchwały nr 2081
Senatu UwB
z dnia 31 maja 2017 r.

PLAN STUDIÓW PODYPLOMOWYCH
obowiązuje od roku akad. 2017/2018

Nazwa jednostki prowadzącej studia podyplomowe Wydział Ekonomii i Zarządzania

Nazwa studiów podyplomowych "Bezpieczeństwo informacji i ochrona danych osobowych w sektorze publicznym"

Plan studiów uchwalony przez Radę Wydziału dnia 4 września 2017 roku

L.P.	NAZWA PRZEDMIOTU	KOD przedmiotu USOS	punkty ECTS	Egz./Zal.	Liczba godzin zajęć						
					RAZEM	WYKŁADY	ĆWICZENIA	KONWERSATORIA	LABORATORIA	SEMINARIA	ZAJĘCIA TERENOWE
1	2	3	4	5	6	7	8	9	10	11	12
	WYKŁAD INAUGURUJĄCY			-	**2**	2					
I.	**MODUŁ I: Obszar ekonomiczny w bezpieczeństwie informacji**		12		**32**	16	16				
1	Podstawy zarządzania w kontekście bezpieczeństwa informacji	0300-SPB-PZBI	1,5	Zaliczenie bez oceny	4	2	2				
2	Stosowanie Normy ISO 27001 w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)	0300-SPB-ISO	3		8	4	4				
3	Audyt SZBI	0300-SPB-ASZBI	3		8	4	4				
4	Planowanie ciągłości działania	0300-SPB-PCD	1,5		4	2	2				
5	Zarządzanie ryzykiem	0300-SPB-ZR	1,5		4	2	2				
6	Zarządzanie incydentami	0300-SPB-ZI	1,5		4	2	2				
II.	**MODUŁ II: Regulacje międzynarodowe, unijne i krajowe w obszarze bezpieczeństwa informacji**		19		**50**	25	25				
1	Ustrój administracji rządowej i samorządowej oraz specyfika jednostek sektora publicznego	0300-SPB-UARS	3		8	4	4				
2	Normy prawa i dobre praktyki w ochronie informacji i danych osobowych	0300-SPB-NPDP	3		8	4	4				
3	Pakiet reformujący ochronę danych osobowych	0300-SPB-PRODO	3		8	4	4				

L.P.	NAZWA PRZEDMIOTU	KOD przedmiotu USOS	punkty ECTS	Egz./Zal.	Liczba godzin zajęć						
					RAZEM	WYKŁADY	ĆWICZENIA	KONWERSATORIA	LABORATORIA	SEMINARIA	ZAJĘCIA TERENOWE
4	Status prawny administratorów bezpieczeństwa informacji/inspektorów ochrony danych, administratorów danych osobowych i procesorów	0300-SPB-SPABI	3	Zaliczenie bez oceny	8	4	4				
5	Organy ochrony danych osobowych	0300-SPB-OODO	1,5		4	2	2				
6	Informacje niejawne (zagadnienia ogólne i rozwiązania praktyczne)	0300-SPB-IN	1,5		4	2	2				
7	Dostęp do informacji publicznej (zagadnienia ogólne i rozwiązania praktyczne)	0300-SPB-DIP	3		8	4	4				
8	Odpowiedzialność w obszarze ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej	0300-SPB-ODPO	1		2	1	1				
III.	**MODUŁ III: Standardy zarządzania bezpieczeństwem informacji: studium przypadków – rozwiązania praktyczne**		8		24	12	12				
1	Realizacja zadań z zakresu ochrony danych osobowych w oparciu o zasoby własne lub outsourcing	0300-SPB-RZODO	1	Zaliczenie bez oceny	4	2	2				
2	Aspekty praktyczne w SZBI	0300-SPB-APSZBI	4		12	6	6				
3	Powierzenie danych osobowych do przetwarzania podmiotom trzecim	0300-SPB-PDO	1,5		4	2	2				
4	Dobre praktyki w SZBI	0300-SPB-DBSZBI	1,5		4	2	2				
IV.	**MODUŁ IV: Kompetencje miękkie w bezpieczeństwie informacji**		8		22	11	11				
1	Czynnik ludzki w bezpieczeństwie informacji	0300-SPB-CLBI	1,5	Zaliczenie bez oceny	4	2	2				
2	Wymiana informacji, dzielenie się wiedzą, samodoskonalenie się	0300-SPB-WIDWS	1,5		4	2	2				
3	Wystąpienia publiczne, w tym narzędzia budowania efektownych prezentacji	0300-SPB-WP	3		8	4	4				
4	Komunikacja a bezpieczeństwo informacji	0300-SPB-KBI	1		4	2	2				
5	Etyka zawodowa w bezpieczeństwie informacji	0300-SPB-EZBI	1		2	1	1				
V.	**MODUŁ V: Rozwiązania techniczno – informatyczne w bezpieczeństwie informacji**		10		28	14	14				
1	Aspekty techniczne w bezpieczeństwie informacji	0300-SPB-ATBI	3		8	4	4				

L.P.	NAZWA PRZEDMIOTU	KOD przedmiotu USOS	punkty ECTS	Egz./Zal.	Liczba godzin zajęć						
					RAZEM	WYKŁADY	ĆWICZENIA	KONWERSATORIA	LABORATORIA	SEMINARIA	ZAJĘCIA TERENOWE
2	Cloud computing w bezpieczeństwie informacji	0300-SPB-CCBI	1	Zaliczenie bez oceny	**2**	1	1				
3	Bezpieczeństwo infrastruktury informatycznej	0300-SPB-BII	1		**4**	2	2				
4	Kryptografia i inne mechanizmy bezpieczeństwa	0300-SPB-KMB	1		**2**	1	1				
5	Cyberterroryzm	0300-SPB-CBTR	1		**2**	1	1				
6	Nowoczesne technologie a ochrona danych osobowych	0300-SPB-NTODO	1		**4**	2	2				
7	Sfera publicznych e-usług	0300-SPB-SPEU	2		**6**	3	3				
	Seminarium dyplomowe oraz obrony	0300-SPB-SD	**3**	Egzamin	**10**					10	
	WYKŁAD KOŃCOWY				**2**	2					
OGÓŁEM			**60**		170						

DZIEKAN
WYDZIAŁU EKONOMII I ZARZĄDZANIA
dr hab. Marzanna Poniatowicz
Prof. UwB
(pieczątka i podpis Dziekana)