Uchwała nr 2405
Senatu Uniwersytetu w Białymstoku
z dnia 25 kwietnia 2019 r.

w sprawie ustalenia programu studiów podyplomowych: Studia Podyplomowe Bezpieczeństwo informacji i ochrona danych osobowych, obowiązującego od roku akademickiego 2019/2020

Na podstawie art. 28 ust. 1 pkt 11 ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2018 r., poz. 1668 z późn. zm.) Senat Uniwersytetu w Białymstoku uchwala, co następuje:

§ 1

1. Senat Uniwersytetu w Białymstoku ustala, obowiązujący od roku akademickiego 2019/2020, program studiów podyplomowych: *Studia Podyplomowe Bezpieczeństwo informacji i ochrona danych osobowych.*
2. Program studiów stanowi Załącznik do niniejszej Uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący
Senatu Uniwersytetu w Białymstoku

Prof. dr hab. Robert W. Ciborowski

Załącznik
do Uchwały nr 2405
Senatu UwB
z dnia 25 kwietnia 2019 r.

EFEKTY UCZENIA SIĘ

Studiów Podyplomowych Bezpieczeństwo Informacji i Ochrona Danych Osobowych

1. **Kwalifikacje nadawane po ukończeniu studiów podyplomowych na poziomie: 7 PRK.**

   Ukończenie podyplomowych studiów Bezpieczeństwo informacji i ochrona danych osobowych 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 inspektora ochrony danych oraz zadań administratora danych osobowych i procesora. Ukończenie studiów podyplomowych Bezpieczeństwo informacji i ochrona danych osobowych będzie stanowiło podstawę do wykazania spełnienia przewidzianych w przepisach prawa wymogów stawianych inspektorowi ochrony danych po dniu 25 maja 2018 roku.

2. **Umiejscowienie studiów w dziedzinie kształcenia *(z uwzględnieniem dziedziny/dziedzin nauki)*: nauki społeczne**
3. **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 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 inspektora ochrony danych w danym podmiocie sektora publicznego i prywatnego, skutecznie zbudować efektywną współpracę inspektora ochrony danych 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.**
4. **Wskazanie, czy w procesie definiowania efektów uczenia się uwzględniono zapotrzebowanie otoczenia społeczno-gospodarczego: W procesie definiowania efektów kształcenia uwzględniono potrzeby organizacji (jednostki sektora publicznego i prywatnego) 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 inspektora ochrony danych osobowych. Uwzględnione zostały również potrzeby administratorów danych osobowych oraz procesorów sektora publicznego i prywatnego.**
5. **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 uczenia się	OPIS ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ Po ukończeniu studiów podyplomowych w następujących obszarach:
WIEDZA, absolwent zna i rozumie:			
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 zaawansowanej wiedzy szczegółowej właściwe dla programu kształcenia główne trendy rozwojowe dyscyplin naukowych lub artystycznych istotnych dla programu kształcenia	SP7_WG01	zakres zadań i kompetencji inspektora ochrony danych, administratora oraz procesora.
		SP7_WG02	modelowy system zarządzania bezpieczeństwem informacji w organizacji.
		SP7_WG03	narzędzia i metody wykonywania zadań inspektora ochrony danych oraz administratora danych osobowych.
		SP7_WG04	obowiązujące regulacje prawne z zakresu ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznych
		SP7_WG05	podstawy zarządzania wiedzą, ciągłością działania, ryzykiem, incydentami w organizacji.
		SP7_WG06	pojęcie audytu bezpieczeństwa informacji, etapy i zasady jego planowania i realizacji.
		SP7_WG07	zakres stosowania normy ISO 27001.
		SP7_WG08	ryzyka w organizacji i analizę ryzyka.
		SP7_WG09	zagadnienia związane z prowadzeniem szkoleń wewnętrznych dla osób przetwarzających dane osobowe.
		SP7_WG10	potrzebę tworzenia, weryfikacji i aktualizacji dokumentacji związanej z ochroną danych osobowych w jednostkach sektora publicznego i prywatnego.
		SP7_WG11	regulacje odnoszące się do informacji niejawnych.
		SP7_WG12	zasady udostępniania informacji publicznej.
		SP7_WG13	kierunki rozwoju e-usług.
P7S _WK	fundamentalne dylematy współczesnej cywilizacji; ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z nadaną kwalifikacją;	SP7_WK01	podstawową terminologię nauk o zarządzaniu, ekonomiczną, prawniczą i informatyczną dotyczącą obszaru ochrony danych osobowych w jednostce sektora publicznego i prywatnego.
		SP7_WK02	podstawy m.in. prawne i finansowe funkcjonowania jednostek sektora publicznego i prywatnego oraz podstawy zarządzania w tych jednostkach.

		SP7_WK03	procesy zachodzące w organizacji wymagające zaangażowania inspektora ochrony danych.
		SP7_WK04	funkcjonowanie systemów informatycznych i nowoczesnych technologii stosowanych w jednostkach administracji publicznej i podmiotach sektora prywatnego.
		SP7_WK05	rolę komunikacji w organizacji i proces przepływu informacji.
		SP7_WK06	istotę oddziaływania kultury organizacyjnej i instrumentów z nią związanych na sprawność i skuteczność zarządzania bezpieczeństwem informacji.
		SP7_WK07	istotę zachowań etycznych i nieetycznych.
		SP7_WK08	wpływ nowoczesnych technologii na ochronę danych osobowych.
UMIEJĘTNOŚCI, absolwent potrafi:			
P7S _UW	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; • dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych (ICT)	SP7_UW01	reagować na incydenty naruszenia procedur związanych z ochroną danych osobowych w organizacji.
		SP7_UW02	interpretować i odpowiednio stosować przepisy prawa z dziedziny ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej.
		SP7_UW03	nadzorować, tworzyć i gromadzić dokumentację z zakresu ochrony danych osobowych wymaganą przepisami prawa.
		SP7_UW04	stosować najistotniejsze zapisy normy ISO 27001
		SP7_UW05	szacować i analizować ryzyka dla systemu bezpieczeństwa informacji, wskazywać możliwości przeciwdziałania im oraz obniżać ich poziom.
		SP7_UW06	korzystać z e-usług.
		SP7_UW07	nadzorować procesy mające związek z ochroną danych osobowych.
P7S _UK	komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców prowadzić debatę	SP7_UK01	planować, przeprowadzać i analizować rozmowy z administratorem danych osobowych oraz procesorem i właścicielami zasobów informacyjnych.
		SP7_UK02	opracować rekomendacje dla organizacji mające na celu podniesienie poziomu zarządzania bezpieczeństwem informacji.
		SP7_UK03	rozróżnić etyczne i nieetyczne zachowania w stosunkach w organizacji mające związek z ochroną danych osobowych i znaleźć sposoby przeciwdziałania nim.

P7S _UO	kierować pracą zespołu	SP7_UO01	rozwijać umiejętność pracy analitycznej i koncepcyjnej.
		SP7_UO02	zaplanować własne działania w celu wykonania obowiązków inspektora ochrony danych.
		SP7_UO03	wskazać korzyści ze stosowania nowoczesnych technologii w organizacji.
		SP7_UO04	rozpoznawać zagrożenia wynikające z nowoczesnych technologii i błędu ludzkiego.
P7S _UU	samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie	SP7_UU01	prowadzić szkolenia wewnętrzne dla personelu z zakresu ochrony danych osobowych.
		SP7_UU02	skutecznie motywować siebie i innych do zdobywania wiedzy.
		SP7_UU03	rozpoznawać style efektywnego uczenia się, aby poprawiać efektywność wykonywanej pracy.
KOMPETENCJE SPOŁECZNE, absolwent jest gotów do:			
P7S _KK	krytycznej oceny posiadanej wiedzy i odbieranych treści uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu	SP7_KK01	pokonywania problemów i trudności wynikających z kontaktów interpersonalnych i hierarchii w organizacji.
		SP7_KK02	własnego wpływu na organizację poprzez kształtowanie i poprawę funkcjonalności systemu zarządzania bezpieczeństwem informacji.
P7S _KO	wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, inicjowania działania na rzecz interesu publicznego, myślenia i działania w sposób przedsiębiorczy	SP7_KO01	samodoskonalenia, podnoszenia własnych kompetencji ważnych w relacjach interpersonalnych i funkcjonowaniu organizacji.
		SP7_KO02	skutecznego motywowania współpracowników, podwładnych.
P7S _KR	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	SP7_KR01	podnoszenia poziom umiejętności budowania relacji interpersonalnych.
		SP7_KR02	podnoszenia poziom umiejętności wystąpień publicznych w zakresie prowadzenia szkoleń.
		SP7_KR03	inspirowania i organizowania procesu uczenia się innych osób.
		SP7_KR04	pracy w zespole, przyjmując w nim różne role.
		SP7_KR05	doskonalenia skutecznych metod komunikacji i negocjacji w wykonywaniu zadań inspektora ochrony danych, administratora danych osobowych, procesora.

PROGRAM STUDIÓW PODYPLOMOWYCH

I. INFORMACJE OGÓLNE

1. Nazwa studiów podyplomowych:

   Studia Podyplomowe Bezpieczeństwo Informacji i Ochrona Danych Osobowych

2. Czas trwania studiów podyplomowych:

   2 semestry

3. Założenia ogólne:

   Założeniem Studia Podyplomowe Bezpieczeństwo informacji i ochrona danych osobowych jest wyposażenie absolwenta w ustrukturyzowaną oraz aktualną wiedzę, a także praktyczne umiejętności z obszarów związanych ze specyfiką zadań wykonywanych przez inspektorów ochrony danych, administratorów danych osobowych, procesorów.

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

   60 punktów

5. Ogólna liczba godzin zajęć dydaktycznych:

   170 godzin

6. Program uchwalony na posiedzeniu Rady Wydziału w dniu ***4 marca 2019 roku*** obowiązuje od ***roku akademickiego 2019/2020***.

II. WYKAZ PRZEDMIOTÓW

Przedmioty	**Punkty ECTS**	**Odniesienie do zakładanych efektów uczenia się**	**Sposób weryfikacji zakładanych efektów uczenia się**
WYKŁAD WPROWADZAJĄCY, 2 godz.			
MODUŁ I: Obszar ekonomiczny w ochronie danych osobowych i bezpieczeństwie informacji 32 godziny, 12 punktów ECTS			
1) Podstawy zarządzania w kontekście bezpieczeństwa informacji	1,5	SP7_WK01, SP7 _WG02, SP7_WK03, SP7 _WG05, SP7_WK06, SP7_UW07, SP7_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).
2) Stosowanie Normy ISO 27001 w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)	3	SP7_WK03, SP7 _WG07, SP7_WK04, SP7_UW04, SP7_KK02, SP7_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	SP7 _WG02, SP7_WK03, SP7_WG06, SP7_UK02, SP7_UK01, SP7_UW07, SP7_KK01, SP7_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	SP7 _WG05, SP7 _WG10, SP7_UO01, SP7_UW01, SP7_UW07, SP7_KK01, SP7_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, SP7 _WG05, SP7 _WG08, SP7_UW05, SP7_UO04, SP7_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	SP7_UW01, SP7_UW03, SP7 _WG05, SP7_UO04, SP7_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	1,5	SP7 _WK01, SP7_WK02, SP7_WK03, SP7_UW02, SP7_KK01, SP7_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).
2) Prawne i ekonomiczne podstawy funkcjonowania sektora prywatnego	1,5	SP7 _WK01, SP7_WK02, SP7_WK03, SP7_UW02, SP7_KK01, SP7_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).
3) Normy prawa i dobre praktyki w ochronie informacji i danych osobowych	3	SP7 _WK01, SP7_WG04, SP7 _WG01, SP7_WG03, SP7 _WG10, SP7_WG11, SP7_UW02, SP7_UW03, SP7_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) Prawne aspekty ochrony danych osobowych	4,5	SP7 _WG01, SP7_WG04, SP7 _WK01, SP7_WG03, SP7_WK06, SP7_UW02, SP7_UW03, SP7_UO01, SP7_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) Status prawny inspektorów ochrony danych, administratorów danych osobowych i procesorów	3	SP7 _WG01, SP7 _WG02, SP7 _WG03, SP7_WG10, SP7_WK03, SP7_UW03, SP7_UO01, SP7_UO02, SP7_UK01, SP7_KK02, SP7_KR01, SP7_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).
6) Organy ochrony danych osobowych	1,5	SP7_WG04, SP7 _WG10, SP7_UW02, SP7_UW03, SP7_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).
7) Informacje niejawne (zagadnienia ogólne i rozwiązania praktyczne) w sektorze publicznym i przedsiębiorstwach	1,5	SP7 _WG11, SP7_WG04, SP7_UW02, SP7_UO01, SP7_KO01, SP7_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) Jawność życia publicznego (zagadnienia ogólne i rozwiązania praktyczne)	1,5	SP7 _WK01, SP7 _WG11, SP7 _WG12, SP7_UW02, SP7_UO01, SP7_KO01, SP7_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).
9) Odpowiedzialność w obszarze ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej	1	SP7 _WK01, SP7 _WG11, SP7_UW02, SP7_UO01, SP7_KK02, SP7_UK03, SP7_KO01, SP7_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	SP7 _WG01, SP7 _WG02, SP7 _WG03, SP7 _WG04, SP7_WK03, SP7_WK06, SP7_UW03, SP7_UK02, SP7_UO02, sP7_UW07, SP7_UK03, SP7_UK01, SP7_KK02, SP7_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	SP7_WG02, SP7_WG03, SP7_WK03, SP7_WK04, SP7_WK06, SP7_WK05, SP7_UW03, SP7_UK02, SP7_UW07, SP7_KK01, SP7_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) Powierzenie danych osobowych do przetwarzania podmiotom trzecim	1,5	SP7 _WG04, SP7_WK01, SP7_WK02, SP7_WK03, SP7 _WG03, SP7_UW02, SP7_UW03, SP7_UO01, SP7_UW07, SP7_KK02, SP7_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	SP7 _WG03, SP7 _WG02, SP7_WK03, SP7_WK04, SP7_WK05, SP7_WK06, SP7_UW03, SP7_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 (obrona pracy).

		SP7_UK02, SP7_KK01, SP7_KR04	
MODUŁ IV: Kompetencje miękkie w bezpieczeństwie informacji 22 godziny, 8 punktów ECTS			
1) Czynnik ludzki w bezpieczeństwie informacji	1,5	SP7_WK05, SP7_UU01, SP7 _WG05, SP7_WK06, SP7_WK07, SP7_UK01, SP7_UK03, SP7_UO04, SP7_KK01, SP7_KO02, SP7_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	SP7 _WG03, SP7_WG05, SP7_WK05, SP7 _WG09, SP7_UK03, SP7_UO01, SP7_UU01, SP7_UU03, SP7_KR01, SP7_KR03, SP7_KO01, SP7_KO02, SP7_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	SP7 _WG03, SP7_WG09, SP7_UU01, SP7_UU02, SP7_UU03, SP7_KO02, SP7_KR02, SP7_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	SP7_WK03, SP7_WK05, SP7_WK06, SP7_UW07, SP7_UK01, SP7_UK03, SP7_KK01, SP7_KK02, SP7_KR01,	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).

		SP7_KR04, SP7_KR05	
5) Etyka zawodowa w bezpieczeństwie informacji	1	SP7_UK03, SP7_WK07, SP7_KK01, SPS_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	2,5	SP7 _WG02, SP7 _WG03, SP7_WK03, SP7_WK04, SP7_WK05, SP7_WK08, SP7_UW07, SP7_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	SP7_WK04, SP7_WK08, SP7 _WG03, SP7_UO03, SP7_UO04, SP7_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	SP7 _WG02, SP7_WG03, SP7_WK03, SP7_WK04, SP7_WK08, SP7_UO03, SP7_UO04, SP7_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	SP7_WG03, SP7 _WG02, SP7_WK03, SP7_WK04, SP7_WK08, SP7_UO03, SP7_UO04, SP7_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	SP7_WG02, SP7_WG03, SP7_WK03, SP7_WK04, SP7_WK08, SP7_UO03, SP7_UO04, SP7_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	SP7 _WG02, SP7 _WG03, SP7_WK03, SP7_WK04, SP7_WK08, SP7_UO03, SP7_UO04, SP7_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 e-usług	2	SP7 _WG03, SP7_WK03, SP7_WK04, SP7_WG13, SP7_WK08, SP7_UO03, SP7_UO02, SP7_UW06, SP7_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 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);

Egzamin (na ostatnim zjeździe).

UNIWERSYTET W BIAŁYMSTOKU

PLAN STUDIÓW PODYPLOMOWYCH
obowiązuje od roku akad. 2019/2020

Nazwa studiów podyplomowych: Studia Podyplomowe Bezpieczeństwo Informacji i Ochrona Danych Osobowych

Plan studiów uchwalony przez Radę Wydziału dnia 04.03.2019 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	0300-SPO-1WW		-	**2**	2					
I.	**MODUŁ I: Obszar ekonomiczny w ochronie danych osobowych i bezpieczeństwie informacji**		12		**32**	16	16				
1	Podstawy zarządzania w kontekście bezpieczeństwa informacji	0300-SPO-1PZB	1,5		**4**	2	2				
2	Stosowanie Normy ISO 27001 w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)	0300-SPO-1ISO	3	Zaliczenie bez oceny	**8**	4	4				
3	Audyt SZBI	0300-SPO-1ASZ	3		**8**	4	4				
4	Planowanie ciągłości działania	0300-SPO-1PCD	1,5		**4**	2	2				
5	Zarządzanie ryzykiem	0300-SPO-1ZR	1,5		**4**	2	2				
6	Zarządzanie incydentami	0300-SPO-1ZI	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-SPO-1UAR	1,5		**4**	2	2				
2	Prawne i ekonomiczne podstawy funkcjonowania sektora prywatnego	0300-SPO-1PESPR'	1,5		**4**	2	2				

L.P.	NAZWA PRZEDMIOTU	KOD przedmiotu USOS	punkty ECTS	Egz./Zal.	Liczba godzin zajęć						
					RAZEM	WYKŁADY	ĆWICZENIA	KONWERSATORIA	LABORATORIA	SEMINARIA	ZAJĘCIA TERENOWE
3	Normy prawa i dobre praktyki w ochronie informacji i danych osobowych	0300-SPO-1NPD	3	Zaliczenie bez oceny	**8**	4	4				
4	Prawne aspekty ochrony danych osobowych	0300-SPO-1PADO'	4,5		**12**	6	6				
5	Status prawny inspektorów ochrony danych, administratorów danych osobowych i procesorów	0300-SPO-1SPA	3		**8**	4	4				
6	Organy ochrony danych osobowych	0300-SPO-1OOD	1,5		**4**	2	2				
7	Informacje niejawne (zagadnienia ogólne i rozwiązania praktyczne) w sektorze publicznym i przedsiębiorstwach	0300-SPO-1IN	1,5		**4**	2	2				
8	Jawność życia publicznego(zagadnienia ogólne i rozwiązania praktyczne)	0300-SPO-1JZP'	1,5		**4**	2	2				
9	Odpowiedzialność w obszarze ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej	0300-SPO-1ODP	1		**2**	1	1				
III.	**MODUŁ III: Standardy zarządzania bezpieczeństwem informacji: studium przypadków – rozwiązania praktyczne**		8	Zaliczenie bez oceny	**24**	12	12				
1	Realizacja zadań z zakresu ochrony danych osobowych w oparciu o zasoby własne lub outsourcing	0300-SPO-1RZO	1		**4**	2	2				
2	Aspekty praktyczne w SZBI	0300-SPO-1APS	4		**12**	6	6				
3	Powierzenie danych osobowych do przetwarzania podmiotom trzecim	0300-SPO-1PDO	1,5		**4**	2	2				
4	Dobre praktyki w SZBI	0300-SPO-1DPS	1,5		**4**	2	2				
IV.	**MODUŁ IV: Kompetencje miękkie w bezpieczeństwie informacji**		8		**22**	11	11				
1	Czynnik ludzki w bezpieczeństwie informacji	0300-SPO-1CLB	1,5		**4**	2	2				

L.P.	NAZWA PRZEDMIOTU	KOD przedmiotu USOS	punkty ECTS	Egz./Zal.	Liczba godzin zajęć						
					RAZEM	WYKŁADY	ĆWICZENIA	KONWERSATORIA	LABORATORIA	SEMINARIA	ZAJĘCIA TERENOWE
2	Wymiana informacji, dzielenie się wiedzą, samodoskonalenie się	0300-SPO-1WID	1,5	Zaliczenie bez oceny	**4**	2	2				
3	Wystąpienia publiczne, w tym narzędzia budowania efektownych prezentacji	0300-SPO-1WPP	3		**8**	4	4				
4	Komunikacja a bezpieczeństwo informacji	0300-SPO-1KBI	1		**4**	2	2				
5	Etyka zawodowa w bezpieczeństwie informacji	0300-SPO-1EZB	1		**2**	1	1				
V.	**MODUŁ V: Rozwiązania techniczno – informatyczne w bezpieczeństwie informacji**		10		**28**	14	14				
1	Aspekty techniczne w bezpieczeństwie informacji	0300-SPO-1ATB	2,5	Zaliczenie bez oceny	**6**	3	3				
2	Cloud computing w bezpieczeństwie informacji	0300-SPO-1CCB	1		**2**	1	1				
3	Bezpieczeństwo infrastruktury informatycznej	0300-SPO-1BII	1		**4**	2	2				
4	Kryptografia i inne mechanizmy bezpieczeństwa	0300-SPO-1KRG	1,5		**4**	2	2				
5	Cyberterroryzm	0300-SPO-1CBT	1		**2**	1	1				
6	Nowoczesne technologie a ochrona danych osobowych	0300-SPO-1NTO	1		**4**	2	2				
7	Sfera e-usług	0300-SPO-1SEUS'	2		**6**	3	3				
	Seminarium oraz egzamin	0300-SPO-1SDO	3	Egzamin	**10**					10	
	WYKŁAD KOŃCOWY	0300-SPO-1WK			**2**	2					
OGÓŁEM			**60**		170	**82**	**78**			**10**	