Załącznik nr 2 do protokołu z posiedzenia Rady Wydziału Ekonomii i Finansów Uniwersytetu w Białymstoku z dnia 17.05.2021r.

UCHWAŁA Nr 38/RW/II/21

Rady Wydziału Ekonomii i Finansów Uniwersytetu w Białymstoku
z dnia 17 maja 2021r.

w sprawie zaopiniowania projektu programu Studiów Podyplomowych Bezpieczeństwo informacji i ochrona danych osobowych, obowiązującego od roku akademickiego 2021/2022

Na podstawie § 59 ust. 1 pkt 6 Statutu Uniwersytetu w Białymstoku Rada Wydziału Ekonomii i Finansów Uniwersytetu w Białymstoku pozytywnie opiniuje projekt programu Studiów Podyplomowych Bezpieczeństwo informacji i ochrona danych osobowych obowiązujący od roku akademickiego 2021/2022, który stanowi załącznik do niniejszej uchwały.

Przewodnicząca
Rady Wydziału Ekonomii i Finansów
Uniwersytetu w Białymstoku

Prof. dr hab. Marzanna Poniatowicz

Załącznik
do Uchwały nr 38/RW/II/21
Rady Wydziału Ekonomii i Finansów
z dnia 17.05.2021 r.

PROGRAM STUDIÓW PODYPLOMOWYCH

Nazwa studiów podyplomowych:

Bezpieczeństwo informacji i ochrona danych osobowych

Obowiązuje od roku akademickiego: 2021/2022

Część I. Informacje ogólne.

1. Nazwa jednostki prowadzącej kształcenie: Wydział Ekonomii i Finansów UwB
2. Ogólne cele kształcenia:
   Głównym celem studiów jest przekazanie specjalistycznej wiedzy teoretycznej i praktycznych umiejętności z zakresu ochrony danych osobowych i zarządzania bezpieczeństwem informacji, niezbędnych do efektywnego, zgodnego z prawem, sprawnego i profesjonalnego wykonywania zadań inspektora ochrony danych, zastępcy inspektora ochrony danych osobowych oraz zadań administratora i podmiotu przetwarzającego.
3. Umiejscowienie studiów w dyscyplinie/dyscyplinach naukowych, do których odnoszą się efekty uczenia się: ekonomia i finanse, nauki o zarządzaniu i jakości, nauki prawne
4. Wskazanie, w jaki sposób w procesie definiowania efektów uczenia się uwzględniono zapotrzebowanie otoczenia społeczno-gospodarczego:
   Studia są odpowiedzią na zapotrzebowanie otoczenia społeczno-gospodarczego na kompleksową wiedzę i profesjonalne umiejętności z zakresu bezpieczeństwa informacji i ochrony danych osobowych, którego wzrost wiąże się z istotną zmianą w prawie – rozpoczęciem obowiązywania rozporządzenia Unii Europejskiej tzw. RODO. W procesie definiowania efektów uczenia się 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. Liczba semestrów: 2
6. Łączna liczba punktów ECTS umożliwiająca ukończenie studiów podyplomowych: 60
7. Łączna liczba godzin zajęć na studiach podyplomowych: 170
8. 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 ochrony danych osobowych i zarządzania bezpieczeństwem informacji w organizacji.

9. Kwalifikacje nadawane po ukończeniu studiów podyplomowych na poziomie: 7
   Zdobyta w czasie studiów wiedza i umiejętności pozwolą absolwentom profesjonalnie wykonywać i organizować własną pracę, ale też przygotować się do wykonywania zadań na stanowisku inspektora ochrony danych i zastępcy inspektora ochrony danych w danym podmiocie tak sektora publicznego jak i prywatnego, skutecznie zbudować efektywną współpracę inspektora ochrony danych i jego zastępcy (jeśli zostanie ustanowiony) z administratorem danych lub podmiotem przetwarzającym, 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.
10. Zaopiniowano na Radzie Wydziału Ekonomii i Finansów w dniu 17 maja 2021 r.

Część II. Efekty uczenia się.

Symbol opisu charakterystyk drugiego stopnia PRK	Symbol efektu uczenia się	Opis efektu uczenia się
Wiedza, absolwent zna i rozumie:		
P7S_WG	SP7_WG1	w pogłębionym stopniu zakres zadań i kompetencji inspektora ochrony danych, administratora oraz procesora
	SP7_WG2	w pogłębionym stopniu wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody w modelowym systemie zarządzania bezpieczeństwem informacji w organizacji
	SP7_WG3	w pogłębionym stopniu metody i teorie wyjaśniające złożone zależności, narzędzia i metody wykonywania zadań inspektora ochrony danych oraz administratora danych osobowych
	SP7_WG4	w pogłębionym stopniu obowiązujące regulacje prawne z zakresu ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznych
	SP7_WG5	w pogłębionym stopniu kluczowe zagadnienia oraz wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej dot. podstaw zarządzania wiedzą, ciągłości działania, ryzyka, incydentów w organizacji
	SP7_WG6	w pogłębionym stopniu metody i teorie wyjaśniające złożone zależności, narzędzia i metody audytu bezpieczeństwa informacji, etapy i zasady jego planowania i realizacji
	SP7_WG7	w pogłębionym stopniu kluczowe zagadnienia oraz wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej dot. zakresu stosowania normy ISO 27001
	SP7_WG8	w pogłębionym stopniu wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności w aspekcie ryzyka w organizacji i analizy ryzyka
	SP7_WG9	w pogłębionym stopniu kluczowe zagadnienia oraz wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej dotyczące zagadnień związanych z prowadzeniem szkoleń wewnętrznych dla osób przetwarzających dane osobowe

	SP7_WG10	w pogłębionym stopniu główne tendencje rozwojowe w zakresie potrzeby tworzenia, weryfikacji i aktualizacji dokumentacji związanej z ochroną danych osobowych w jednostkach sektora publicznego i prywatnego
	SP7_WG11	w pogłębionym stopniu regulacje odnoszące się do informacji niejawnych
	SP7_WG12	w pogłębionym stopniu wybrane fakty, obiekty i zjawiska, metody i teorie wyjaśniające zasady udostępniania informacji publicznej
	SP7_WG13	w pogłębionym stopniu główne tendencje rozwojowe w zakresie kierunków rozwoju e-usług
P7S_WK	SP7_WK1	ekonomiczne, prawne, etyczne i inne uwarunkowania ochrony danych osobowych w jednostce sektora publicznego i prywatnego
	SP7_WK2	fundamentalne dylematy w zakresie podstaw m.in. prawnych i finansowych funkcjonowania jednostek sektora publicznego i prywatnego oraz podstaw zarządzania w tych jednostkach
	SP7_WK3	ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów procesów zachodzących w organizacji wymagające zaangażowania inspektora ochrony danych
	SP7_WK4	zasady tworzenia i rozwoju oraz funkcjonowania systemów informatycznych i nowoczesnych technologii stosowanych w jednostkach administracji publicznej i podmiotach sektora prywatnego
	SP7_WK5	ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej, w szczególności rolę komunikacji w organizacji i proces przepływu informacji
	SP7_WK6	ekonomiczne, prawne, etyczne i inne uwarunkowania oddziaływania kultury organizacyjnej i instrumentów z nią związanych na sprawność i skuteczność zarządzania bezpieczeństwem informacji
	SP7_WK7	fundamentalne dylematy dotyczące istoty zachowań etycznych i nieetycznych w organizacji
	SP7_WK8	podstawowe zasady tworzenia i rozwoju oraz wpływu nowoczesnych technologii na ochronę danych osobowych
Umiejętności, absolwent potrafi:		
P7S_UW	SP7_UW1	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, w tym reagować na incydenty naruszenia procedur związanych z ochroną danych osobowych w organizacji
	SP7_UW2	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, w tym interpretować i odpowiednio stosować przepisy prawa z dziedziny ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej
	SP7_UW3	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie

		wykonywać zadania w nieprzewidywalnych warunkach, w tym nadzorować, tworzyć i gromadzić dokumentację z zakresu ochrony danych osobowych wymaganą przepisami prawa
	SP7_UW4	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, w tym stosować najistotniejsze zapisy normy ISO 27001
	SP7_UW5	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, w tym szacować i analizować ryzyka dla systemu bezpieczeństwa informacji, wskazywać możliwości przeciwdziałania im oraz obniżać ich poziom
	SP7_UW6	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, w tym korzystać z e-usług
	SP7_UW7	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, w tym nadzorować procesy mające związek z ochroną danych osobowych
P7S_UK	SP7_UK1	komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców, a w szczególności planować, przeprowadzać i analizować rozmowy z administratorem danych osobowych oraz procesorem i właścicielami zasobów informacyjnych
	SP7_UK2	wykorzystywać posiadaną wiedzę i opracować rekomendacje dla organizacji mające na celu podniesienie poziomu zarządzania bezpieczeństwem informacji
	SP7_UK3	formułować i rozwiązywać złożone i nietypowe problemy, w tym rozróżnić etyczne i nieetyczne zachowania w stosunkach w organizacji mające związek z ochroną danych osobowych i znaleźć sposoby przeciwdziałania nim
P7S_UO	SP7_UO1	współdziałać z innymi osobami w ramach prac zespołowych, rozwijać umiejętność pracy analitycznej i koncepcyjnej
	SP7_UO2	współdziałać z innymi osobami oraz zaplanować własne działania w celu wykonania obowiązków inspektora ochrony danych
	SP7_UO3	podejmować wiodącą rolę w ramach prac zespołowych, wspólnych dyskusji, wskazując korzyści ze stosowania nowoczesnych technologii w organizacji
	SP7_UO4	podejmować wiodącą rolę w zespołach i rozpoznawać zagrożenia wynikające z nowoczesnych technologii i błędu ludzkiego
P7S_UU	SP7_UU1	ukierunkowywać innych w zakresie uczenia się przez całe życie, prowadząc szkolenia wewnętrzne dla personelu z zakresu ochrony danych osobowych

	SP7_UU2	samodzielnie planować uczenie się, skutecznie motywować siebie i innych do zdobywania wiedzy
	SP7_UU3	realizować własne uczenie się, rozpoznawać style efektywnego uczenia się, aby poprawiać efektywność wykonywanej pracy
Kompetencje społeczne, absolwent jest gotów do:		
P7S_KK	SP7_KK1	uznawania znaczenia wiedzy w rozwiązywaniu problemów i trudności wynikających z kontaktów interpersonalnych i hierarchii w organizacji
	SP7_KK2	krytycznej oceny posiadanej wiedzy i odbieranych treści oraz własnego wpływu na organizację poprzez kształtowanie i poprawę funkcjonalności systemu zarządzania bezpieczeństwem informacji
P7S_KO	SP7_KO1	samodoskonalenia, podnoszenia własnych kompetencji ważnych w relacjach interpersonalnych i funkcjonowaniu organizacji
	SP7_KO2	wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, skutecznego motywowania współpracowników, podwładnych
P7S_KR	SP7_KR1	odpowiedzialnego pełnienia ról zawodowych, podnoszenia poziomu umiejętności budowania relacji interpersonalnych
	SP7_KR2	rozwijania dorobku zawodu, podnoszenia poziomu umiejętności wystąpień publicznych w zakresie prowadzenia szkoleń
	SP7_KR3	uwzględniania zmieniających się potrzeb społecznych, w tym inspirowania i organizowania procesu uczenia się innych osób
	SP7_KR4	podtrzymywania etosu zawodu, pracy w zespole, przyjmując w nim różne role
	SP7_KR5	przestrzegania i rozwijania zasad etyki zawodowej, doskonalenia skutecznych metod komunikacji i negocjacji w wykonywaniu zadań inspektora ochrony danych, administratora danych osobowych, procesora

Część III. Opis procesu prowadzącego do uzyskania efektów uczenia się.

Przedmioty	**Odniesienie do zakładanych efektów uczenia się**	**Sposób weryfikacji zakładanych efektów uczenia się**	**Treści programowe zapewniające uzyskanie efektów uczenia się**
Podstawy zarządzania w kontekście bezpieczeństwa informacji	SP7_WK1, SP7_WG2, SP7_WK3, SP7_WG5, SP7_WK6, SP7_UW7, SP7_KK2	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie słuchaczom zakresu oraz narzędzi zarządzania w organizacji, podstawowych funkcji zarządzania, uświadomienie znaczenia

			sprawnego i skutecznego działania w ramach organizacji.
Stosowanie Normy ISO 27001 w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)	SP7_WK3, SP7_WG7, SP7_WK4, SP7_UW4, SP7_KK2, SP7_KR4	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z treścią Normy ISO 27001.
Audyt SZBI	SP7_WG2, SP7_WK3, SP7_WG6, SP7_UK2, SP7_UK1, SP7_UW7, SP7_KK1, SP7_KR4	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie słuchaczom wiedzy i kształtowanie umiejętności w zakresie planowania, przygotowania, prowadzenia audytu zarządzania bezpieczeństwem informacji, zbierania dowodów i raportowania wyników.
Planowanie ciągłości działania	SP7_WG5, SP7 _WG10, SP7_UO1, SP7_UW1, SP7_UW7, SP7_KK1, SP7_KK2	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie istoty zapewnienia ciągłości działania organizacji, podejścia modelowego i organizacyjnego.
Zarządzanie ryzykiem	SP7_WK3, SP7_WG5, SP7 _WG8, SP7_UW5, SP7_UO4, SP7_KK1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z istotą, procedurą oraz narzędziami zarządzania ryzykiem w organizacji.
Zarządzanie incydentami	SP7_UW1, SP7_UW3, SP7_WG5, SP7_UO4, SP7_KK1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy na temat wykrywania incydentów, reagowania, dokumentowania incydentów, działań naprawczych i zapobiegawczych.
Ustrój administracji rządowej i samorządowej oraz specyfika jednostek sektora publicznego	SP7_WK1, SP7_WK2, SP7_WK3, SP7_UW2, SP7_KK1, SP7_KK2	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z zagadnieniami dotyczącymi funkcjonowania administracji publicznej, kompetencji jst, specyfiki przetwarzania

			danych w sektorze publicznym.
Prawne i ekonomiczne podstawy funkcjonowania sektora prywatnego	SP7_WK1, SP7_WK2, SP7_WK3, SP7_UW2, SP7_KK1, SP7_KK2	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie zagadnień dotyczących sektora prywatnego – pojęcia przedsiębiorcy, uczestnictwa przedsiębiorców w obrocie, umów w obrocie gospodarczym.
Normy prawa i dobre praktyki w ochronie informacji i danych osobowych	SP7_WK1, SP7_WG4, SP7_WG1, SP7_WG3, SP7 _WG10, SP7_WG11, SP7_UW2, SP7_UW3, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zaznajomienie słuchaczy z regulacjami prawa krajowego, prawa Unii Europejskiej i prawa międzynarodowego dot. ochrony danych osobowych, oraz dobrymi praktykami dotyczącymi przetwarzania danych.
Prawne aspekty ochrony danych osobowych	SP7_WG1, SP7_WG4, SP7_WK1, SP7_WG3, SP7_WK6, SP7_UW2, SP7_UW3, SP7_UO1, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy na temat przetwarzania danych osobowych w poszanowaniu obowiązujących aktów prawnych.
Prawna i organizacyjna specyfika ochrony danych osobowych w wybranych sektorach (e-commerce, oświata, sektor medyczny i ubezpieczeniowy)	SP7_WG1, SP7_WG2, SP7_WG3, SP7_WG10, SP7_WK3, SP7_UW3, SP7_UO1, SP7_UO2, SP7_UK1, SP7_KK2, SP7_KR1, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie specyfiki przetwarzania danych w różnych sektorach, w tym e-commerce, oświacie, sektorze medycznym i ubezpieczeniowym.
Status prawny inspektorów ochrony danych, administratorów danych osobowych i podmiotów przetwarzających oraz organy ochrony danych osobowych	SP7_WG1, SP7_WG2, SP7_WG3, SP7_WG10, SP7_WK3, SP7_UW3,	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie zadań inspektora ochrony danych osobowych, kompetencji organu nadzorczego ds. ochrony danych osobowych,

	SP7_UO1, SP7_UO2, SP7_UK1, SP7_KK2, SP7_KR1, SP7_KR5		obowiązków administratorów danych i podmiotów przetwarzających.
Informacje niejawne (zagadnienia ogólne i rozwiązania praktyczne) w sektorze publicznym i przedsiębiorstwach	SP7 _WG11, SP7_WG4, SP7_UW2, SP7_UO1, SP7_KO1, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy na temat zasad oraz podstaw prawnych systemu ochrony informacji niejawnych, stosowanych procedur w sytuacjach ich zagrożenia.
Jawność życia publicznego (zagadnienia ogólne i rozwiązania praktyczne)	SP7_WK1, SP7 _WG11, SP7 _WG12, SP7_UW2, SP7_UO1, SP7_KO1, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z zagadnieniem informacji publicznej, udostępniania informacji publicznej bez naruszania prywatności osób.
Odpowiedzialność w obszarze ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej	SP7_WK1, SP7 _WG11, SP7_UW2, SP7_UO1, SP7_KK2, SP7_UK3, SP7_KO1, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie odpowiedzialności karnej, administracyjnej, cywilnej i pracowniczej, ich podstaw, sankcji.
Realizacja zadań z zakresu ochrony danych osobowych w oparciu o zasoby własne lub outsourcing	SP7_WG1, SP7_WG2, SP7_WG3, SP7_WG4, SP7_WK3, SP7_WK6, SP7_UW3, SP7_UK2, SP7_UO2, SP7_UW7, SP7_UK3, SP7_UK1, SP7_KK2, SP7_KR4	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z zadaniami administratora w zakresie ochrony danych osobowych realizowanych samodzielnie oraz przez podmioty zewnętrzne
Aspekty praktyczne w SZBI	SP7_WG2, SP7_WG3, SP7_WK3, SP7_WK4,	Zaliczenie na ocenę. Aktywne uczestnictwo	Omówienie tworzenia, wdrażania i nadzorowania Systemu Bezpieczeństwa

	SP7_WK6, SP7_WK5, SP7_UW3, SP7_UK2, SP7_UW7, SP7_KK1, SP7_KR4	w zajęciach	Informacji w organizacji, w tym praktycznych sposobów pozwalających spełniać wymogi SZBI.
Powierzenie danych osobowych do przetwarzania podmiotom trzecim	SP7_WG4, SP7_WK1, SP7_WK2, SP7_WK3, SP7_WG3, SP7_UW2, SP7_UW3, SP7_UO1, SP7_UW7, SP7_KK2, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie konstrukcji powierzenia przetwarzania danych osobowych, roli administratora i podmiotu przetwarzającego, elementów umowy powierzenia przetwarzania danych osobowych.
Dobre praktyki w SZBI	SP7_WG3, SP7_WG2, SP7_WK3, SP7_WK4, SP7_WK5, SP7_WK6, SP7_UW3, SP7_UW7, SP7_UK2, SP7_KK1, SP7_KR4	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z dobrymi praktykami dedykowanymi do stosowania w SZBI, zaprezentowanie warsztatu pracy i metodyki IOD.
Czynnik ludzki w bezpieczeństwie informacji	SP7_WK5, SP7_UU1, SP7_WG5, SP7_WK6, SP7_WK7, SP7_UK1, SP7_UK3, SP7_UO4, SP7_KK1, SP7_KO2, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy na temat psychologicznych mechanizmów ulegania niechcianym wpływom, nieświadomego ujawniania poufnych informacji
Wymiana informacji, dzielenie się wiedzą, samodoskonalenie się	SP7_WG3, SP7_WG5, SP7_WK5, SP7_WG9, SP7_UK3, SP7_UO1, SP7_UU1,	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy w zakresie znaczenia i formy skutecznego dzielenia się wiedzą, wymieniani informacji w organizacji i samodoskonalenia się,

	SP7_UU3, SP7_KR1, SP7_KR3, SP7_KO1, SP7_KO2, SP7_KR4		stosowania narzędzi komunikacji i motywacji.
Wystąpienia publiczne, w tym narzędzia budowania efektownych prezentacji	SP7_WG3, SP7_WG9, SP7_UU1, SP7_UU2, SP7_UU3, SP7_KO2, SP7_KR2, SP7_KR3	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy na temat spójności przekazu, metod angażowania słuchaczy, narzędzi budowania efektownej prezentacji.
Komunikacja a bezpieczeństwo informacji	SP7_WK3, SP7_WK5, SP7_WK6, SP7_UW7, SP7_UK1, SP7_UK3, SP7_KK1, SP7_KK2, SP7_KR1, SP7_KR4, SP7_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy i umiejętności na temat efektywnego przekazywania informacji przy zachowaniu ich bezpieczeństwa.
Etyka zawodowa w bezpieczeństwie informacji	SP7_UK3, SP7_WK7, SP7_KK1, SPS_KR5	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie zasad wynikających z etyki pracy inspektorów ochrony danych, praktyczne wyjaśnienie metod pracy IOD.
Aspekty techniczne w bezpieczeństwie informacji	SP7_WG2, SP7_WG3, SP7_WK3, SP7_WK4, SP7_WK5, SP7_WK8, SP7_UW7, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z metodami przeciwdziałania zagrożeniom związanym z bezpieczeństwem informacji.
Cloud computing w bezpieczeństwie informacji	SP7_WK4, SP7_WK8, SP7_WG3, SP7_UO3, SP7_UO4, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie zagadnienia cloud computingu, usług chmurowych, zagrożeń i zabezpieczeń danych w chmurze obliczeniowej.
Bezpieczeństwo infrastruktury informatycznej	SP7 _WG2, SP7_WG3,	Zaliczenie na ocenę.	Przekazanie wiedzy dotyczącej incydentów,

	SP7_WK3, SP7_WK4, SP7_WK8, SP7_UO3, SP7_UO4, SP7_KO1	Aktywne uczestnictwo w zajęciach	zarządzania incydentami, zespołów reagujących na incydenty.
Kryptografia i inne mechanizmy bezpieczeństwa	SP7_WG3, SP7_WG2, SP7_WK3, SP7_WK4, SP7_WK8, SP7_UO3, SP7_UO4, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Przekazanie wiedzy na temat narzędzi kryptograficznych, zapoznanie z mechanizmami kryptograficznymi.
Cyberterroryzm	SP7_WG2, SP7_WG3, SP7_WK3, SP7_WK4, SP7_WK8, SP7_UO3, SP7_UO4, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Zapoznanie słuchaczy z ewolucją zjawisk zagrożeń w cyberprzestrzeni, rodzajami ataków cyberterrorystycznych, sposobami przeciwdziałania im.
Nowoczesne technologie a ochrona danych osobowych	SP7_WG2, SP7_WG3, SP7_WK3, SP7_WK4, SP7_WK8, SP7_UO3, SP7_UO4, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie wpływu nowoczesnych technologii na zmieniającą się dynamikę zagrożeń, nowoczesnych zabezpieczeń technologicznych i organizacyjnych.
Sfera e-usług	SP7_WG3, SP7_WK3, SP7_WK4, SP7_WG13, SP7_WK8, SP7_UO3, SP7_UO2, SP7_UW6, SP7_KO1	Zaliczenie na ocenę. Aktywne uczestnictwo w zajęciach	Omówienie miejsca i roli e-usług we współczesnym społeczeństwie informacyjnym, zapoznanie z teorią i praktyką funkcjonowania e-usług.
Bezpieczne i higieniczne warunki kształcenia		Zaliczenie.	Zasady bezpiecznych i higienicznych warunków kształcenia

Wymiar, zasady i formę odbywania praktyk zawodowych oraz liczbę punktów ECTS, jaką uczestnik studiów podyplomowych musi uzyskać w ramach tych praktyk, jeżeli program studiów podyplomowych przewiduje realizację praktyk.

Nie dotyczy

Sposoby weryfikacji i oceny efektów uczenia się osiągniętych przez uczestnika studiów podyplomowych w trakcie całego cyklu kształcenia.

Weryfikacja obejmuje wszystkie kategorie obszarów (wiedza, umiejętności i kompetencje społeczne) poprzez: zaliczenia zajęć w ramach poszczególnych modułów (np. aktywność, test, projekt, referat itp.); poprzez i przygotowanie do egzaminu końcowego, a finalnie w trakcie egzaminu dyplomowego.

Warunki ukończenia studiów podyplomowych oraz sposób określenia wyniku studiów podyplomowych na świadectwie ukończenia studiów podyplomowych.

Warunkiem ukończenia studiów podyplomowych jest uzyskanie pozytywnej oceny w zakresie przewidzianych efektów uczenia się, co potwierdzone zostaje zaliczeniem przez prowadzących w ramach poszczególnych zajęć, jak i ostatecznie podczas egzaminu końcowego zdawanego przed komisją składającą się ze specjalistów w zakresie ochrony danych osobowych w wymiarze teoretycznym i praktycznym. Świadectwo ukończenia studiów podyplomowych zawiera informację o stopniu uzyskanym przez Słuchacza.

Objaśnienia oznaczeń:
P6, P7, P8 – poziom PRK
S – charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego

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

Opis procesu prowadzącego do uzyskania efektów uczenia się.
Harmonogram realizacji programu studiów podyplomowych

L.P.	NAZWA ZAJĘĆ	KOD ZAJĘĆ USOS	punkty ECTS	Egzamin / Zaliczenie	Liczba godzin zajęć						
					RAZEM	WYKŁADY	ĆWICZENIA	KONWERSATORIA	LABORATORIA	SEMINARIA	ZAJĘCIA TERENOWE
1	2	3	4	5	6	7	8	9	10	11	12
1	**WYKŁAD INAUGURUJĄCY**	330-SPO-1WW		-	**2**	2					
2	**WYKŁAD Bezpieczne i higieniczne warunki kształcenia (BHP)**	330-SPO-1BHWK		ZAL	**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	330-SPO-1PZB	1,5		**4**	2	2				
2	Stosowanie Normy ISO 27001 w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)	330-SPO-1ISO	3	ZAL	**8**	4	4				
3	Audyt SZBI	330-SPO-1ASZ	3		**8**	4	4				
4	Planowanie ciągłości działania	330-SPO-1PCD	1,5		**4**	2	2				
5	Zarządzanie ryzykiem	330-SPO-1ZR	1,5		**4**	2	2				
6	Zarządzanie incydentami	330-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	330-SPO-1UAR	1,5		**4**	2	2				
2	Prawne i ekonomiczne podstawy funkcjonowania sektora prywatnego	330-SPO-1PESPR'	1,5		**4**	2	2				
3	Normy prawa i dobre praktyki w ochronie informacji i danych osobowych	330-SPO-1NPD	3		**8**	4	4				
4	Prawne aspekty ochrony danych osobowych	330-SPO-1PADO'	4,5		**12**	6	6				
5	Prawna i organizacyjna specyfika ochrony danych osobowych w wybranych sektorach (e-commerce, oświata, sektor medyczny i ubezpieczeniowy)	330-SPO-1SPA	3	ZAL	**8**	4	4				
6	Status prawny inspektorów ochrony danych, administratorów danych osobowych i podmiotów przetwarzających oraz organy ochrony danych osobowych	330-SPO-1OOD	1,5		**4**	2	2				
7	Informacje niejawne (zagadnienia ogólne i rozwiązania praktyczne) w sektorze publicznym i przedsiębiorstwach	330-SPO-1IN	1,5		**4**	2	2				
8	Jawność życia publicznego (zagadnienia ogólne i rozwiązania praktyczne)	330-SPO-1JZP'	1,5		**4**	2	2				
9	Odpowiedzialność w obszarze ochrony danych osobowych, informacji niejawnych i dostępu do informacji publicznej	330-SPO-1ODP	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	330-SPO-1RZO	1	ZAL	4	2	2				
2	Aspekty praktyczne w SZBI	330-SPO-1APS	4		12	6	6				
3	Powierzenie danych osobowych do przetwarzania podmiotom trzecim	330-SPO-1PDO	1,5		4	2	2				
4	Dobre praktyki w SZBI	330-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	330-SPO-1CLB	1,5		4	2	2				
2	Wymiana informacji, dzielenie się wiedzą, samodoskonalenie się	330-SPO-1WID	1,5		4	2	2				
3	Wystąpienia publiczne, w tym narzędzia budowania efektownych prezentacji	330-SPO-1WPP	3	ZAL	8	4	4				
4	Komunikacja a bezpieczeństwo informacji	330-SPO-1KBI	1		4	2	2				
5	Etyka zawodowa w bezpieczeństwie informacji	330-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	330-SPO-1ATB	2,5		6	3	3				
2	Cloud computing w bezpieczeństwie informacji	330-SPO-1CCB	1		2	1	1				
3	Bezpieczeństwo infrastruktury informatycznej	330-SPO-1BII	1		4	2	2				
4	Kryptografia i inne mechanizmy bezpieczeństwa	330-SPO-1KRG	1,5	ZAL	4	2	2				
5	Cyberterroryzm	330-SPO-1CBT	1		2	1	1				
6	Nowoczesne technologie a ochrona danych osobowych	330-SPO-1NTO	1		4	2	2				
7	Sfera e-usług	330-SPO-1SEUS'	2		6	3	3				
	Seminarium oraz obrony	330-SPO-1SDO	3	Egzamin	**8**					**8**	
	WYKŁAD KOŃCOWY	330-SPO-1WK			**2**	2					
OGÓŁEM			**60**		**170**	**84**	**78**			**8**	