

Program studiów podyplomowych

Ogólna charakterystyka studiów podyplomowych	
Wydział prowadzący studia podyplomowe:	Wydział Nauk Historycznych
Nazwa studiów podyplomowych:	Studia podyplomowe studia w zakresie kancelarii tajnej i ochrony informacji niejawnych
Nazwa studiów podyplomowych w j. angielskim:	Postgraduate Diploma Studies in Secret Archives and the Security of Classified Information
Umiejscowienie studiów w obszarze kształcenia:	Zakres studiów mieści się w obszarze nauk humanistycznych. W procesie kształcenia specjalisty z zakresu kancelarii tajnej i ochrony informacji niejawnej niezbędne jest także osiągnięcie wybranych efektów kształcenia z obszaru nauk społecznych, które stanowią uzupełnienie programu.
Kierunek studiów prowadzony przez UMK związany z obszarem kształcenia:	Archiwistyka i zarządzanie dokumentacją
Liczba semestrów:	2
Łączna liczba godzin zajęć dydaktycznych:	210 godz.
Łączna liczba punktów ECTS:	60
Cel studiów podyplomowych: (należy: określić, do czego przygotowują słuchaczy studia podyplomowe – z uwzględnieniem wymogów organizacji zawodowych i pracodawców; opisać uzyskiwane przez słuchaczy nowe uprawnienia i kwalifikacje zawodowe niezbędne na rynku pracy)	Celem studiów jest dostarczenie niezbędnej wiedzy, umiejętności i kompetencji w zakresie profesjonalnego i zawodowego kierowania kancelarią tajną oraz ochroną informacji niejawnej. W programie studiów położono nacisk na praktyczne zaznajomienie słuchacza z funkcjonowaniem kancelarii tajnej, organizowaniem jej pracy, prowadzeniem ewidencji, tworzeniem i znakowaniem dokumentacji niejawnej, organizowaniem polityki bezpieczeństwa i ochrony informacji niejawnej. Wiedza z zakresu podstaw historii i ustroju Polski pozwoli na lepsze wykorzystanie kompetencji w zakresie funkcjonowania administracji w Polsce oraz zasad organizowania kancelarii tajnych. Program studiów obejmuje także zagadnienia związane z podstawową wiedzą i umiejętnościami z archiwistyki i zarządzania dokumentacją, co

	<p>ma duże znaczenie w zakresie postępowania z dokumentacją niejawną, jej przechowywaniem, opracowywaniem, udostępnianiem oraz archiwizowaniem i niszczeniem. W ramach zajęć przybliżone zostaną także zasady funkcjonowania systemów informatycznych, których znajomość jest wykorzystywana przy organizowaniu bezpieczeństwa teleinformatycznego. Nabiera to szczególnego znaczenia w kontekście społeczeństwa informacyjnego, w którym właściwa, profesjonalna ochrona informacji odgrywa coraz istotniejszą rolę. Wykształcenie tych kompetencji wymaga realizacji interdyscyplinarnego programu nauczania z zakresu nauk informacyjnych i nauk o bezpieczeństwie podpartego wiedzą z informatyki, archiwistyki i zarządzania dokumentacją.</p>
<p>Wskazanie związku programu studiów podyplomowych z misją i strategią Wydziału:</p>	<p>Program studiów pozostaje w związku z misją i strategią Wydziału Nauk Historycznych na lata 2011–2020 (cel strategiczny B.2.3. Rozwój różnorodnych form kształcenia ustawicznego) oraz Uniwersytetu, a zwłaszcza z celami kierunkowymi z obszaru „Kształcenie” zapisanymi w „Strategii UMK na lata 2011–2020”. Program studiów ma charakter nowatorski, tj. uwzględnia potrzeby rynku pracy oraz oczekiwania instytucji zainteresowanych zarówno profesjonalnym kierowaniem kancelarią tajną, wykwalifikowanymi pracownikami kancelarii niejawnych jak również profesjonalną ochroną informacji.</p>
<p>Wskazanie, czy w procesie określania efektów kształcenia i rozwiązań programowych uwzględniono opinie interesariuszy zewnętrznych i wewnętrznych:</p>	<p>Informacja jest obecnie cennym towarem, zabieganie o nią staje się celem samym w sobie i prowadzi do wykształcenia się grup, które zawodowo zajmują się jej ochroną, zdobywaniem czy handlowaniem. Bezpieczeństwo informacji jest nie tylko normą i koniecznością, ale także obowiązkiem dla wszystkich instytucji działających w strukturach administracji publicznej oraz firm i organizacji o innym statusie. Wymogi prawa nakładają obowiązek podjęcia działań o charakterze organizacyjnym i technicznym w zakresie bezpieczeństwa informacji, szczególnie tych objętych specjalną ochroną prawną. Współczesne prawo w Polsce dostosowane do standardów przyjętych przez NATO i Unię Europejską, wymaga m.in. konieczności wdrażania w każdej placówce publicznej Polityki Bezpieczeństwa Informacji na podstawie Ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych oraz organizowania kancelarii tajnych i niejawnych w określonych ustawowo jednostkach, w oparciu o akty wykonawcze do Ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Cele powyższe można osiągnąć dzięki ciągłemu podnoszeniu kwalifikacji pracowników zatrudnionych</p>

	przy tworzeniu, gromadzeniu, przechowywaniu, przetwarzaniu i udostępnianiu informacji. Istnieje duże zapotrzebowanie na wykwalifikowanych pracowników kancelarii jawnych i tajnych, urzędników świadomych odnośnie do potrzeby ochrony informacji, zarówno w instytucjach cywilnych, jak i służbach mundurowych. Współcześnie Polityka Bezpieczeństwa Informacji jest jednym z elementów kultury przedsiębiorstwa, którą tworzą i przestrzegają wszyscy pracownicy i współpracownicy.
Efekty kształcenia dla studiów podyplomowych*	
Symbol	Po ukończeniu studiów podyplomowych absolwent osiąga następujące efekty kształcenia:
WIEDZA	
EK_W01	Ma podstawową wiedzę na temat dokumentacji współczesnej, typów i form dokumentacji oraz sposobów ich powstawania
EK_W02	Zna podstawową terminologię z nauk informacyjnych, nauk o zarządzaniu oraz zarządzania dokumentacją; ma uporządkowaną wiedzę na temat kancelarii tajnej oraz ochrony informacji niejawnych.
EK_W03	Ma uporządkowaną wiedzę o współczesnych potrzebach w zakresie wdrażania polityki bezpieczeństwa informacji w aspekcie różnorodnych zagrożeń dla informacji; ma usystematyzowaną wiedzę na temat zagrożeń dla danych osobowych.
EK_W04	Ma podstawową wiedzę o wpływie wydarzeń historyczno-kulturowych na rozwój systemów informatycznych oraz konieczności zapewnienia ich bezpieczeństwa.
EK_W05	Ma uporządkowaną wiedzę na temat gromadzenia, przechowywania, opracowywania i udostępniania dokumentacji niejawnej; na temat funkcjonowania zasobów informacyjnych w jednostkach organizacyjnych oraz archiwach historycznych.
EK_W06	Ma uporządkowaną wiedzę dotyczącą norm prawnych regulujących funkcjonowanie kancelarii tajnych oraz organizowanie polityki bezpieczeństwa i ochrony informacji.
EK_W07	Zna i rozumie elementarne pojęcia i zasady z zakresu prawa autorskiego; ma uporządkowaną wiedzę dotyczącą planowania, organizowania, kontrolowania i motywowania dotyczącą gromadzenia, przechowywania, przetwarzania i udostępniania informacji w jednostce organizacyjnej.
EK_W08	Ma uporządkowaną wiedzę na temat nowoczesnych technologii informacyjno-komunikacyjnych.
EK_W09	Zna podstawowe normy i instrumenty (prawne, organizacyjne i etyczne) będące podstawą do ochrony danych osobowych oraz ich źródła i naturę.
EK_W10	Ma podstawową wiedzę o powiązaniach archiwistyki z zarządzaniem dokumentacją oraz tych dwóch nauk z naukami o zarządzaniu, naukami historycznymi i nauką o informacji.
EK_W11	Zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu prostych zadań z zakresu bezpieczeństwa teleinformatycznego.

EK_W12	Zna i rozumie normy prawne regulujące proces obiegu informacji i dokumentacji w jednostce organizacyjnej, zasady organizowania procesu archiwizacji i brakowania dokumentacji niejawnej; zna i rozumie normy prawne regulujące funkcjonowanie zasobów informacyjnych oraz kancelarii tajnej w jednostce organizacyjnej
UMIEJĘTNOŚCI	
EK_U01	Potrafi wyszukiwać, analizować, oceniać, selekcjonować i użytkować informacje z zakresu zarządzania informacją, nauk informacyjnych, nauk o zarządzaniu z wykorzystaniem różnych źródeł i sposobów oraz formułować na tej podstawie krytyczne sądy.
EK_U02	Posiada podstawowe umiejętności, obejmujące formułowanie i analizę problemów, dobór metod i narzędzi, dobór i wyszukiwanie specjalistycznej literatury, opracowanie i prezentację wyników, pozwalające na rozwiązywanie problemów z zakresu bezpieczeństwa teleinformatycznego.
EK_U03	Potrafi rozpoznać i analizować różne rodzaje zagrożeń dla informacji.
EK_U04	Potrafi ocenić przydatność różnorodnych rozwiązań organizacyjnych kancelarii tajnej dla efektywnego zarządzania informacją niejawną w jednostce organizacyjnej oraz wybrać i zastosować właściwy sposób postępowania; zdefiniować i ocenić zasady i instrumenty ochrony danych osobowych.
EK_U05	Potrafi rozpoznawać i analizować różne rodzaje i typy dokumentacji współczesnej, umie tworzyć i znakować dokumenty niejawne, umie zorganizować proces archiwizacji i brakowania dokumentacji niejawnej
EK_U06	Posiada umiejętność rozpoznawania problemów i potrzeb społecznych w zakresie bezpieczeństwa informacji oraz potrafi projektować ich rozwiązanie w oparciu o metody właściwe dla nauki o bezpieczeństwie oraz nauki informacyjne
EK_U07	Umie interpretować i wykorzystywać akty prawne będące podstawą do ochrony danych osobowych.
EK_U08	Potrafi zaprojektować politykę bezpieczeństwa informacji.
EK_U09	Potrafi rozpoznać i ocenić przydatność poznanych środowisk programistycznych i narzędzi komputerowych do realizacji prostych zadań inżynierskich z zakresu bezpieczeństwa teleinformatycznego.
EK_U10	Potrafi wykorzystywać źródła przepisów prawnych obowiązujących obecnie, regulujących zasady pracy współczesnych instytucji w zakresie zarządzania informacją, w tym informacją niejawną w kancelarii tajnej.
EK_U11	Umie interpretować i stosować polskie i międzynarodowe akty prawne odnoszące się do tworzenia, przechowywania, przekazywania i udostępniania dokumentacji niejawnej; umie interpretować i stosować przepisy odnoszące się do archiwizacji i brakowania dokumentacji niejawnej.
KOMPETENCJE SPOŁECZNE	
EK_K01	Rozumie i docenia znaczenie wiedzy w życiu człowieka, potrafi samodzielnie i krytycznie uzupełniać wiedzę i umiejętności; potrafi inspirować i organizować proces uczenia się innych osób wykorzystując do tego celu możliwości wynikające z osobistych predyspozycji oraz nabytej wiedzy i umiejętności.
EK_K02	Ma elementarne umiejętności organizacyjne pozwalające na realizację celów związanych z projektowaniem i podejmowaniem działań w zakresie ochrony zasobu informacyjnego i bezpieczeństwa teleinformatycznego.
EK_K03	Potrafi określać priorytety służące realizacji określonych przez siebie lub innych zadań w zakresie przechowywania i ochrony zasobów informacyjnych, zagrożeń dla informacji i ich zapobieganiu, archiwizacji i brakowania dokumentacji niejawnej, samodzielnie inicjuje i podejmuje różnorodne zadania.
EK_K04	Prawidłowo identyfikuje i rozstrzyga dylematy związane z tworzeniem, gromadzeniem, przechowywaniem, przetwarzaniem i udostępnianiem dokumentacji niejawnej, ochroną informacji oraz bezpieczeństwem teleinformatycznym; potrafi dokonać analizy własnych działań w zakresie dokumentacji niejawnej i wskazać ewentualne obszary wymagające modyfikacji w

	przyszłości.
EK_K05	Akceptuje zasady etyczne pożądane w zawodzie specjalisty z zakresu ochrony informacji.
EK_K06	Ma świadomość odpowiedzialności za zachowanie dziedzictwa kulturowego (zwłaszcza archiwalnego) regionu, kraju, Europy; rozumie i dostrzega potrzebę jego promowania.
EK_K07	Kieruje się profesjonalnym zachowaniem i zasadami etyki zawodowej na stanowisku pracy związanym z zarządzaniem informacją.

Moduły kształcenia wraz z zakładanymi efektami kształcenia

Moduły kształcenia	Przedmioty	Liczba punktów ECTS	Charakter zajęć (teoretyczne/ praktyczne) T/P	Zakładane efekty kształcenia	Sposób weryfikacji zakładanych efektów kształcenia osiągniętych przez słuchacza
Moduł kształcenia I: Kurs kierownika kancelarii tajnej	Kancelaria tajna	6	P	EK_W02; EK_W12; EK_U04; EK_U10; EK_K02; EK_K03	przygotowanie krótkiej pracy pisemnej
	Dokumentacja niejawna	5	P	EK_W01; EK_W05; EK_U05; EK_U11; EK_K04; EK_K06	przygotowanie projektu dokumentu niejawnego ze znakowaniem
	Postępowanie z informacją niejawną	4	P	EK_W05; EK_W12; EK_U05; EK_U10; EK_K02; EK_K03	przygotowanie krótkiej pracy pisemnej
	Archiwizacja i brakowanie dokumentacji niejawnej	4	P	EK_W05; EK_W12; EK_U05; EK_U11; EK_K03; EK_K04	przygotowanie projektów protokołów archiwizacji i zniszczenia dokumentacji niejawnej

	Zarządzanie informacją w jednostce organizacyjnej	4	T	EK_W02; EK_W07; EK_W12; EK_U01; EK_U10; EK_K01; EK_K07	egzamin pisemny z treści prezentowanych w toku zajęć
Moduł kształcenia II. Bezpieczeństwo informacji niejawnych	Administrator Bezpieczeństwa Informacji	4	T/P	EK_W02; EK_W03; EK_U06; EK_U07; EK_K02; EK_K04	przygotowanie krótkiej pracy pisemnej
	Przechowywanie i ochrona zasobu informacji niejawnych	4	T	EK_W06; EK_W12; EK_U04; EK_U10; EK_K02; EK_K03	egzamin pisemny z treści prezentowanych w toku zajęć
	Polityka bezpieczeństwa informacji	4	T/P	EK_W06; EK_W07; EK_U04; EK_U08; EK_K01; EK_K05	egzamin pisemny z treści prezentowanych w toku zajęć
	Zasady i instrumenty ochrony danych osobowych	3	T/P	EK_W03; EK_W11; EK_U04; EK_U07; EK_K05; EK_K07	przygotowanie krótkiej pracy pisemnej
	Bezpieczeństwo teleinformatyczne	4	P	EK_W04; EK_W08; EK_W11; EK_U02; EK_U09; EK_K02; EK_K04	przygotowanie krótkiej analizy bezpieczeństwa informacji wybranej strony WWW

Moduł kształcenia III. Archiwalno-kancelaryjny	Podstawy historii i ustroju Polski po II wojnie światowej	4	T	EK_W03; EK_W08; EK_U02; EK_U06; EK_K01; EK_K03	przygotowanie krótkiej pracy pisemnej
	Wprowadzenie do archiwistyki i zarządzania dokumentacją	4	T/P	EK_W02; EK_W10; EK_W12; EK_U01; EK_U04; EK_K01; EK_K05	przygotowanie krótkiej pracy pisemnej
Moduł kształcenia IV. Projekt dyplomowy		10	P	EK_W02; EK_W03; EK_U01; EK_U02; EK_U08; EK_K01; EK_K03	Przygotowanie pracy pisemnej na ustalony temat

Program studiów obowiązuje od semestru zimowego roku akademickiego 2016/2017

Program studiów został uchwalony na posiedzeniu Rady Wydziału Nauk Historycznych w dniu 17 MAJ 2016 r.
(nazwa wydziału) (data posiedzenia rady wydziału)

DZIEKAN
Wydziału Nauk Historycznych

..... prof. dr hab. Józef Gzella
(podpis Dziekana)

***Objaśnienia oznaczeń:**

- EK - efekty kształcenia
- W – kategoria wiedzy
- U – kategoria umiejętności
- K – kategoria kompetencji społecznych
- 01, 02, 03, etc. – numer efektu kształcenia

** W przypadku, gdy studia podyplomowe realizowane są wspólnie przez kilka wydziałów, program studiów musi być podpisany przez dziekanów wszystkich współpracujących wydziałów i wskazywać daty posiedzeń poszczególnych rad wydziałów.