Uchwała Nr 0012.35.II.2024
Senatu Uniwersytetu Kaliskiego im. Prezydenta Stanisława Wojciechowskiego
z dnia 27 września 2024 roku

w sprawie ustalenia programu studiów podyplomowych Bezpieczeństwo informacyjne organizacji

Na podstawie art. 28 ust. 1 pkt 11 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2023 r., poz. 742 ze zm.) uchwala się, co następuje:

§ 1

Ustala się program studiów podyplomowych Bezpieczeństwo informacyjne organizacji, w brzmieniu załącznika do uchwały.

§ 2

Program studiów podyplomowych, o którym mowa w § 1, obowiązuje od cyklu kształcenia 2024/2025.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Senatu Uniwersytetu Kaliskiego
im. Prezydenta Stanisława Wojciechowskiego
Rektor

prof. dr hab. n. med. i n. o zdr. Andrzej Wojtyła

Opracowała: mgr Anna Szymańska

RADCA PRAWNY
Aleksandra Mazek
PZ-3351

Załącznik do Uchwały Nr 0012.35.II.2024

Senatu Uniwersytetu Kaliskiego z dnia 27.09.2024 r.

Uniwersytet Kaliski

im. Prezydenta Stanisława Wojciechowskiego

PROGRAM STUDIÓW PODYPLOMOWYCH

Bezpieczeństwo informacyjne organizacji

obowiązuje od cyklu kształcenia 2024/2025

I. INFORMACJE OGÓLNE	
Jednostka organizacyjna prowadząca studia	Wydział Nauk Społecznych
Nawa studiów podyplomowych	**Bezpieczeństwo informacyjne organizacji**
Nazwa dziedziny/dyscypliny	Nauki społeczne/ nauki o bezpieczeństwie
Typ studiów	Studia podyplomowe - doskonalenie kwalifikacji zawodowych
Język, w którym prowadzone są studia podyplomowe	Język polski
Informacje ogólne, forma, czas trwania	Studia podyplomowe „Bezpieczeństwo informacyjne organizacji" realizowane są przez Wydział Nauk Społecznych w ramach współpracy Instytutem Nauk o Bezpieczeństwie oraz Centrum Badawczo-Wdrożeniowym. Prowadzone są w formie niestacjonarnej i trwają dwa semestry. Program obejmuje łącznie **274 godziny** zajęć dydaktycznych, realizowanych podczas **dwudniowych zjazdów (sobota–niedziela)**. Program zakłada realizację części zjazdów (głównie wykładów) w formule pracy zdalnej z wykorzystaniem metod i technik kształcenia na odległość.
Forma zakończenia studiów	Ukończenie studiów następuje po zaliczeniu wszystkich przedmiotów objętych programem (formę zaliczenia ustalają prowadzący), uzyskaniu 60 punktów ECTS oraz złożeniu i obronie projektu/pracy dyplomowej. Formę pracy ustala się indywidualnie (artykuł, esej, projekt, opracowanie naukowe innego typu). Przewiduje się możliwość publikacji najlepszych prac dyplomowych w tematycznym numerze czasopisma naukowego lub w postaci wydawnictwa zwartego (w wydawnictwie naukowym). Ukończenie studiów potwierdzone jest świadectwem ukończenia studiów podyplomowych.
Adresaci studiów	Studia adresowane są do: • absolwentów kierunków społecznych i humanistycznych pierwszego i drugiego stopnia, szczególnie informatycznych, bezpieczeństwa wewnętrznego, bezpieczeństwa narodowego, zarządzania, studiów MISH i interdyscyplinarnych; • absolwentów kierunku bezpieczeństwo wewnętrzne, bezpieczeństwo narodowe, zarządzania, chcących zdobyć nowe kompetencje i specjalizację w badaniach bezpieczeństwa informacyjnego organizacji; • inspektorów, projektantów i menadżerów systemu bezpieczeństwa działających w różnych sektorach przemysłu i administracji; • pracowników samorządów związanych z ustawowymi zadaniami gmin w zakresie bezpieczeństwa informacyjnego; • pracowników jednostek administracji publicznej oraz organizacji pozarządowych pracujących nad poprawieniem zasad bezpieczeństwa informacyjnego swoich jednostek; • szefów, kierowników, specjalistów bezpieczeństwa informatycznego instytucji państwowych i firm prywatnych; • pracowników organizacji (firm) zajmujących się rozwiązywaniem problemów bezpieczeństwa informacyjnego; • wszystkich osób zainteresowanych interdyscyplinarnym poszerzeniem swojej wiedzy i doświadczeń w zakresie bezpieczeństwa informacyjnego organizacji, rozwojem kompetencji kreatywnych i pisania tekstów naukowych o bezpieczeństwie informacyjnym organizacji w sposób krytyczny. Słuchaczami studiów podyplomowych mogą być osoby, które posiadają dyplom ukończenia studiów wyższych pierwszego lub

	drugiego stopnia albo jednolitych studiów magisterskich i uzyskały decyzję o przyjęciu na studia podyplomowe.
Koncepcja i cele kształcenia oraz opis zdobywanych kwalifikacji	Bezpieczeństwo informacyjne, w odróżnieniu od bezpieczeństwa informacji, jest pojęciem złożonym i dużo trudniejszym do uchwycenia. Bezpieczeństwo informacji najczęściej ogranicza się do spełnienia trzech atrybutów informacji takich jak: poufność, dostępność i integralność. Osiągane jest w trzech obszarach: organizacyjnym, technicznym i fizycznym poprzez implementację systemu zarządzania bezpieczeństwem informacji bazującym na przyjętych normach, np. ISO 27001. Bezpieczeństwo informacyjne wykracza w istotny sposób poza ramy obowiązujących norm. Informacja funkcjonująca w przestrzeni informacyjnej, której cyberprzestrzeń jest tylko jednym z elementów, stała się narzędziem i środkiem realizacji przyjętych celów działania. W bezpieczeństwie informacyjnym, oprócz zapewnienia bezpieczeństwa informacji, niezwykle istotne jest stosowanie elementów walki informacyjnej, w tym szeroko rozumianej propagandy i dezinformacji. Jej umiejętne wykorzystanie pozwala nie tylko na działanie z pozycji dodatniej w stosunku do potencjalnych przeciwników np. podczas negocjacji, ale także pozwala kreować rzeczywistość stawiającą dany podmiot zarówno w korzystnym, jak i niekorzystnym świetle. Co więcej, musimy być równocześnie świadomi, że także my możemy być celem oddziaływania informacyjnego, celem dezinformacji, propagandy, nie tylko białej czy szarej, ale także czarnej, ukierunkowanej na dyskredytację, zmniejszenie wpływów, poniesienie wymiernych strat. Z tego też względu niezwykle istotnego znaczenia nabiera zdolność skutecznego przeciwstawienia się wrogiej kampanii informacyjnej i identyfikacji, kto za nią stoi. Studia podyplomowe „Bezpieczeństwo informacyjne organizacji" stanowią intersującą ofertę edukacyjną odpowiadającą na zapotrzebowanie rynku pracy. Wychodząc poza typową wiedzę o zarządzaniu informacją i systemach bezpieczeństwa kierunek oferuje interdyscyplinarne podejście do poznawania, badania, opisywania i rozumienia bezpieczeństwa informacyjnego w szerszej perspektywie. Zapewnia spojrzenie na zagadnienia z perspektywy szerokiego ujęcia nowoczesnych aspektów wykorzystania informacji w mediach, komunikowaniu się, planowaniu strategicznym czy też tworzenie pozytywnego wizerunku biznesowego w social mediach. Studia pozwolą słuchaczom nie tylko lepiej zrozumieć i poznać wszelakie aspekty bezpieczeństwa informacyjnego w organizacji, ale i umożliwią samodzielną pracę badawczą, rozwój horyzontów myślowych i realizację własnych projektów zapewniających efektywniejsze wykorzystanie systemów bezpieczeństwa informacyjnego. Celem studiów jest poszerzenie kompetencji osób o kierunkowym wykształceniu pierwszego lub drugiego stopnia (informatycznym, informacyjnym, bezpieczeństwa wewnętrznego, bezpieczeństwa narodowego, zarządzania i innych) o specjalistyczną wiedzę z zakresu bezpieczeństwa informacyjnego organizacji oraz umiejętności i kompetencje w zakresie metodologii badań naukowych w obszarze bezpieczeństwa informacyjnego. Dodatkowym celem kierunku jest umożliwienie w przystępnej formie wszystkim zainteresowanym (po ukończeniu studiów pierwszego lub drugiego stopnia różnych kierunków) nabycia wiedzy i umiejętności mających zastosowanie w pracy inspektorów, projektantów, menadżerów lub pracowników zajmujących się bezpieczeństwem informatycznym w różnych organizacjach w kraju i zagranicą.
Poziom Polskiej Ramy Kwalifikacji nadawany po ukończeniu studiów	poziom 7

podyplomowych	
Nazwa instytucji współpracujących	Instytut Nauk o Bezpieczeństwie Centrum Badawczo-Wdrożeniowe
Wymagania wstępne	Na studia podyplomowe mogą być przyjęci kandydaci posiadający dyplom ukończenia studiów co najmniej pierwszego stopnia (tj. legitymujący się co najmniej tytułem zawodowym licencjata lub inżyniera potwierdzonym odpowiednim dyplomem).
Kadra dydaktyczna studiów podyplomowych	Zajęcia prowadzone będą przez nauczycieli akademickich oraz specjalistów z określonych dziedzin
Plan studiów podyplomowych	Załącznik 1
Matryca efektów uczenia się	Załącznik 2

II. OPIS EFEKTÓW UCZENIA SIĘ Z ODNIESIENIAMI DO CHARAKTERYSTYK DRUGIEGO STOPNIA PRK ORAZ CHARAKTERYSTYK UNIWERSALNYCH

EFEKTY UCZENIA SIĘ DLA KIERUNKU
Bezpieczeństwo informacyjne organizacji

Symbole stosowane :

EUP- efekt uczenia się dla studiów podyplomowych

Wiedza: absolwent zna i rozumie

P7S_WG – Zakres i głębia - kompletność perspektywy poznawczej i zależności

P7S_WK – Kontekst - uwarunkowania, skutki

Umiejętności: absolwent potrafi

P7S_UW – Wykorzystanie wiedzy - rozwiązywane problemy i wykonywane zadania

P7S_UK – Komunikowanie się - odbieranie i tworzenie wypowiedzi, upowszechnianie wiedzy w środowisku naukowym i posługiwanie się językiem obcym

P7S_UO – Organizacja pracy - planowanie i pracę zespołową

P7S_UU – Uczenie się - planowanie własnego rozwoju i rozwoju innych osób

Kompetencje społeczne: absolwent jest gotów do:

P7S_KK – Oceny - krytyczne podejście

P7S_KO – Odpowiedzialność - wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego

P7S_KR – Rola zawodowa - niezależność i rozwój etosu

Symbol efektów uczenia się dla programu studiów podyplomowych	**Efekty uczenia się dla kierunku studiów**	Odniesienie do charakterystyk drugiego stopnia PRK poziom 7 i charakterystyk uniwersalnych
	WIEDZA:	
EUP_W01	zna i rozumie główne problemy związane z zarządzaniem systemem bezpieczeństwa informacyjnego w organizacji, zna i rozumie metody zarządzenia systemem bezpieczeństwa organizacji; rozumie zasadność stosowania socjotechniki w zarządzaniu bezpieczeństwem informacji w organizacji;	P7S_WG P7S_WK P7U_W
EUP_W02	wymienia i omawia kluczowe kierunki współczesnych metod, teorii i praktyk badawczych w zakresie bezpieczeństwa informacyjnego w ujęciu interdyscyplinarnym, przydatne w pracy w organizacjach zajmujących się wykorzystaniem informacji, efektami jej użycia;	P7S_WG P7S_WK P7U_W
EUP_W03	w pogłębionym stopniu wyjaśnia i przedstawia sposoby opracowania i zastosowania koncepcji strategii i polityki bezpieczeństwa informacyjnego, odnosząc je do wiedzy o ryzyku, audycie i zagrożeniach dla lepszej realizacji działań naprawczych w organizacji;	P7S_WG P7S_WK P7U_W
EUP_W04	zna i rozumie podstawowe zasady wykorzystania prawa z zakresu bezpieczeństwa i ochrony informacji; zna system prawnej ochrony informacji i danych osobowych w Polsce i UE; zna i rozumnie problemy odpowiedzialności kryminalnej związane z bezpieczeństwem informacyjnym w organizacji;	P7S_WG P7S_WK P7U_W
EUP_W05	ma wiedzę o fundamentalnych dylematach cywilizacji, szczególnie w odniesieniu to teleinformatyki i jej bezpieczeństwa; ma wiedzę o czynnikach i kierunkach zmian, jakie zachodzą w praktyce oraz teoriach bezpieczeństwa informacyjnego oraz konsekwencjach	P7S_WK P7U_W

	tych zmian;	
UMIEJĘTNOŚCI:		
EUP_U01	potrafi identyfikować zjawiska w środowisku bezpieczeństwa informacyjnego będące jego zagrożeniami, kryzysami lub szansami dla bezpieczeństwa podmiotów przetwarzających informację; potrafi samodzielnie analizować jakość informacji poprzez wyszukiwanie, selekcjonowanie i ewaluację źródeł informacji z zastosowaniem metod i technik w środowisku technologiczno-informacyjnym;	P7S_UW P7U_U
EUP_U02	posiada umiejętność twórczego projektowania badań naukowych z zakresu bezpieczeństwa informacyjnego (prognozowanie, analizowanie procesów występujących w systemie bezpieczeństwa informacyjnego, wnioskowanie) oraz oddziaływających na nie wydarzeń, czynników czy faktów;	P7S_UW P7U_U
EUP_U03	potrafi wykorzystywać informacje do prognozowania i rozwiązywania problemów; potrafi analizować, dedukować i indukować wnioski z uzyskanej wiedzy i praktyk. Potrafi określać potencjał, relacyjność i istotność wydarzeń związanych z bezpieczeństwem informacyjnym; potrafi wykorzystywać uzyskane informacje na potrzeby polityki bezpieczeństwa informacyjnego;	P7S_UW P7S_UK P7U_U
EUP_U04	potrafi przygotowywać i prowadzić wystąpienia publiczne różnych typów, przekazując wiedzę specjalistyczną z zakresu bezpieczeństwa informacyjnego, zagrożeń informatycznych, bezpieczeństwa teleinformatycznego o różnorodnym przygotowaniu;	P7S_UK P7U_U
EUP_U05	ma zdolność projektowania badań naukowych z zakresu bezpieczeństwa informacyjnego, poszerzania własnych kompetencji i uczenia się nowych zagadnień oraz komunikowania wyników badań poprzez pisanie tekstów różnych form, wyposażonych w warsztat badawczy;	P7S_UU P7U_U
KOMPETENCJE SPOŁECZNE:		
EUP_K01	jest otwarta/otwarty na nowe rozwiązania, zdolny do zmiany opinii wobec rzeczowej i rzetelnej argumentacji; okazuje dbałość i determinację w samodzielnym wyszukiwaniu i ewaluowaniu źródeł wiedzy i informacji z obszaru bezpieczeństwa informacyjnego;	P7S_KK P7U_K
EUP_K02	potrafi analizować sytuacje w środowisku bezpieczeństwa informacyjnego, określać samodzielnie kierunki rozwoju polityki bezpieczeństwa i precyzować zasadne projekty dla bezpieczeństwa informacyjnego;	P7S_KO P7U_K
EUP_K03	potrafi analitycznie i rzetelnie ocenić efektywność własnej pracy, pracy zespołu oraz stopień zaangażowania i zaawansowania w zadanie;	P7S_KR P7U_K

EUP_K04	potrafi samodzielnie formułować propozycje i rozwiązania sytuacji problemowych, kryzysowych na podstawie analizy i oceny sytuacji i wydarzeń; potrafi konkretyzować pomysły, myśleć i działać w sposób zgodny z interesami organizacji, podejmować decyzje przedsiębiorcze i pozytywne dla interesu organizacji;	P7S_KO P7U_K
EUP_K05	jest gotowa/gotów do postępowania zgodnego z normami etycznymi oraz prawnymi w nauce i działalności zawodowej, w tym do ich propagowania w rolach społecznych i zawodowych;	P7S_KR P7U_K

Załącznik nr 1

PLAN STUDIÓW „BEZPIECZEŃSTWO INFORMACYJNE ORGANIZACJI”

SEMESTR I

Przedmioty	Liczba punktów ECTS	Liczba godzin teoretycznych	Liczba godzin praktycznych	Forma kształcenia	Forma zaliczenia
Podstawy zarządzania bezpieczeństwem informacji	4	15		Wykład	EGZ
Zarządzanie ryzykiem	4		15	Konwersatorium	ZAL
Socjotechnika w zarządzaniu bezpieczeństwem informacji	4	15		Wykład	ZAL
Ochrona informacji w wymiarze narodowym i sojuszniczym	2	10		Wykład	ZAL
Wybrane problemy kryminalistyki Przestępstwa komputerowe	2		10	Konwersatorim	ZAL
Audyt wewnętrzny i zewnętrzny	2		10	Konwersatorium	ZAL
Gra decyzyjna	6		30	Konwersatorium	ZAL
Walka, wojna i operacje informacyjne	2	10		Wykład	EGZ
Oblicza współczesnej propagandy, dezinformacji i manipulacji	2	10		Konwersatorium	ZAL
Elementy komunikowania strategicznego w biznesie	2		10	Ćwiczenia	ZAL
Szkolenie bhp-zajecia obowiazkowe dodatkowe	0	4		Szkolenie	ZAL
RAZEM SEMESTR I	**30**	**64**	75	-	-

SEMESTR II

Przedmioty	Liczba punktów ECTS	Liczba godzin teoretycznych	Liczba godzin praktycznych	Forma kształcenia	Forma zaliczenia
Praktyczne metody zarządzania systemem bezpieczeństwa informacji	2		10	Konwersatorium	ZAL
Współczesne zagrożenia dla bezpieczeństwa informacji	6		20	Konwersatorium	ZAL

Uwarunkowania prawne ochrony informacji	2	10		Wykład	EGZ
Prawne aspekty bezpieczeństwa systemów teleinformatycznych	2	10		Konwersatorium	ZAL
Polityka bezpieczeństwa informacji	2	10		Wykład	EGZ
Tworzenie strategii i polityk bezpieczeństwa informacyjnego	5	10	10	Konwersatorium	ZAL
Wyostrzanie social mediów w biznesie	5		20	Ćwiczenia	ZAL
Kontrola strategiczna	2		10	Konwersatorium	ZAL
Seminarium dyplomowe	4		15	Seminarium	ZAL
RAZEM SEMESTR II	**30**	**50**	**85**	**-**	**-**

RAZEM SEMESTR I i II	**60**	**114**	**160**	**274**	**-**

Załącznik nr 2.

MATRYCA EFEKTÓW UCZENIA SIĘ dla studiów podyplomowych Bezpieczeństwo informacyjne organizacji

Symbol efektów uczenia się dla programu studiów podyplomowych	Efekt uczenia się dla programu studiów podyplomowych		PRZEDMIOTY																		
		Podstawy zarządzania bezpieczeństwem informacji	Zarządzanie ryzykiem	Praktyczne metody zarządzania systemem bezpieczeństwa informacji	Socjotechnika w zarządzaniu bezpieczeństwem informacji	Współczesne zagrożenia dla bezpieczeństwa informacji	Uwarunkowania prawne ochrony informacji	Ochrona informacji w wymiarze narodowym i sojuszniczym	Wybrane problemy kryminalistyki Przestępstwa komputerowe	Prawne aspekty bezpieczeństwa systemów teleinformatycznych	Polityka bezpieczeństwa informacji	Audyt wewnętrzny i zewnętrzny	Tworzenie strategii i polityk bezpieczeństwa informacyjnego	Gra decyzja	Walka, wojna i operacje informacyjne	Oblicza współczesnej propagandy, dezinformacji i manipulacji.	Elementy komunikowania strategicznego w biznesie	Wyostrzanie social mediów w biznesie	Kontrola strategiczna	Seminarium dyplomowe	
		WIEDZA																			
EUP_ W01	zna i rozumie główne problemy związane z zarządzaniem bezpieczeństwa informacyjnego w organizacji, zna i rozumie metody zarządzenia systemem bezpieczeństwa organizacji; rozumie zasadność stosowania socjotechniki w zarządzaniu bezpieczeństwem informacji w organizacji;	+	+	+	+	+					+		+	+	+	+	+		+	+	
EUP_ WO2	wymienia i omawia kluczowe kierunki współczesnych metod, teorii i praktyk badawczych w zakresie bezpieczeństwa informacyjnego w ujęciu interdyscyplinarnym, przydatne w pracy w organizacjach zajmujących się wykorzystaniem informacji, efektami jej użycia;			+	+						+	+		+					+		+
EUP- W03	w pogłębionym stopniu wyjaśnia i przedstawia sposoby opracowania i zastosowania koncepcji strategii i politykach bezpieczeństwa informacyjnego, odnosząc je do wiedzy o ryzyku, audycie i zagrożeniach dla lepszej realizacji działań naprawczych w organizacji;		+			+						+	+	+								

Symbol efektów uczenia się dla programu studiów podyplomowych	Efekt uczenia się dla programu studiów podyplomowych	PRZEDMIOTY																		
		Podstawy zarządzania bezpieczeństwem informacji	Zarządzanie ryzykiem	Praktyczne metody zarządzania systemem bezpieczeństwa informacji	Socjotechnika w zarządzaniu bezpieczeństwem informacji	Współczesne zagrożenia dla bezpieczeństwa informacji	Uwarunkowania prawne ochrony informacji	Ochrona informacji w wymiarze narodowym i sojuszniczym	Wybrane problemy kryminalistyki Przestępstwa komputerowe	Prawne aspekty bezpieczeństwa systemów teleinformatycznych	Polityka bezpieczeństwa informacji	Audyt wewnętrzny i zewnętrzny	Tworzenie strategii i polityk bezpieczeństwa informacyjnego	Gra decyzja	Walka, wojna i operacje informacyjne	Oblicza współczesnej propagandy, dezinformacji i manipulacji.	Elementy komunikowania strategicznego w biznesie	Wyostrzanie social mediów w biznesie	Kontrola strategiczna	Seminarium dyplomowe	
EUP_W04	zna i rozumie podstawowe zasady wykorzystania prawa z zakresu bezpieczeństwa i ochrony informacji; zna system prawnej ochrony informacji i danych osobowych w Polsce i UE; zna i rozumnie problemy odpowiedzialności kryminalnej związane z bezpieczeństwem informacyjnym w organizacji						+	+	+	+									+	+	
EUP_W05	Ma wiedzę o fundamentalnych dylematach cywilizacji, szczególnie w odniesieniu to teleinformatyki i jej bezpieczeństwa; ma wiedzę o czynnikach i kierunkach zmian, jakie zachodzą w praktyce oraz teoriach bezpieczeństwa informacyjnego oraz konsekwencjach tych zmian;													+	+	+	+	+		+	
	UMIEJĘTNOŚCI																				
EUP_U01	Potrafi identyfikować zjawiska w środowisku bezpieczeństwa informacyjnego będące jego zagrożeniami, kryzysami lub szansami dla bezpieczeństwa podmiotów przetwarzających informację; potrafi samodzielnie analizować jakość informacji poprze wyszukiwanie, selekcjonowanie i ewaluację źródeł informacji z zastosowaniem metod i technik w środowisku technologiczno-informacyjnym;	+	+	+	+	+		+								+		+	+	+	

Symbol efektów uczenia się dla programu studiów podyplomowych	Efekt uczenia się dla programu studiów podyplomowych		PRZEDMIOTY																	
		Podstawy zarządzania bezpieczeństwem informacji	Zarządzanie ryzykiem	Praktyczne metody zarządzania systemem bezpieczeństwa informacji	Socjotechnika w zarządzaniu bezpieczeństwem informacji	Współczesne zagrożenia dla bezpieczeństwa informacji	Uwarunkowania prawne ochrony informacji	Ochrona informacji w wymiarze narodowym i sojuszniczym	Wybrane problemy kryminalistyki Przestępstwa komputerowe	Prawne aspekty bezpieczeństwa systemów teleinformatycznych	Polityka bezpieczeństwa informacji	Audyt wewnętrzny i zewnętrzny	Tworzenie strategii i polityk bezpieczeństwa informacyjnego	Gra decyzja	Walka, wojna i operacje informacyjne	Oblicza współczesnej propagandy, dezinformacji i manipulacji.	Elementy komunikowania strategicznego w biznesie	Wyostrzanie social mediów w biznesie	Kontrola strategiczna	Seminarium dyplomowe	
EUP_U02	posiada umiejętność twórczego projektowania badań naukowych z zakresu bezpieczeństwa informacyjnego (prognozowanie, analizowanie procesów występujących w systemie bezpieczeństwa informacyjnego, wnioskowanie) oraz oddziaływających na nie wydarzeń, czynników czy faktów;;			+					+			+		+		+	+	+		+	
EUP_U03	Potrafi wykorzystywać informacje do prognozowania i rozwiązywania problemów; potrafi analizować, dedukować i indukować wnioski z uzyskanej wiedzy i praktyk. Potrafi określać potencjał, relacyjność i istotność wydarzeń związanych z bezpieczeństwem informacyjnym; potrafi wykorzystywać na potrzeby polityki bezpieczeństwa informacyjnego uzyskane informacje				+	+	+				+		+	+		+	+	+	+	+	
EUP_U04	potrafi przygotowywać i prowadzić wystąpienia publiczne różnych typów, przekazując wiedzę specjalistyczną z zakresu bezpieczeństwa informacyjnego, zagrożeń informatycznych, bezpieczeństwa teleinformatycznego o różnorodnym przygotowaniu;		+		+							+			+					+	

Symbol efektów uczenia się dla programu studiów podyplomowych	Efekt uczenia się dla programu studiów podyplomowych	PRZEDMIOTY																			
		Podstawy zarządzania bezpieczeństwem informacji	Zarządzanie ryzykiem	Praktyczne metody zarządzania systemem bezpieczeństwa informacji	Socjotechnika w zarządzaniu bezpieczeństwem informacji	Współczesne zagrożenia dla bezpieczeństwa informacji	Uwarunkowania prawne ochrony informacji	Ochrona informacji w wymiarze narodowym i sojuszniczym	Wybrane problemy kryminalistyki Przestępstwa komputerowe	Prawne aspekty bezpieczeństwa systemów teleinformatycznych	Polityka bezpieczeństwa informacji	Audyt wewnętrzny i zewnętrzny	Tworzenie strategii i polityk bezpieczeństwa informacyjnego	Gra decyzja	Walka, wojna i operacje informacyjne	Oblicza współczesnej propagandy, dezinformacji i manipulacji.	Elementy komunikowania strategicznego w biznesie	Wyostrzanie social mediów w biznesie	Kontrola strategiczna	Seminarium dyplomowe	
EUP_U05	ma zdolność projektowania badań naukowych z zakresu bezpieczeństwa informacyjnego, poszerzania własnych kompetencji i uczenia się nowych zagadnień oraz komunikowania wyników badań poprzez pisanie tekstów różnych form, wyposażonych w warsztat badawczy;		+	+	+				+		+	+		+						+	+	
	KOMPETENCJE SPOŁECZNE																				
EUP_K01	Jest otwarty na nowe rozwiązania, zdolny do zmiany opinii wobec rzeczowej i rzetelnej argumentacji; okazuje dbałość i determinację w samodzielnym wyszukiwaniu i ewaluowaniu źródeł wiedzy i informacji z obszaru bezpieczeństwa informacyjnego;	+		+				+					+		+			+	+	+	
EUP_K02	Potrafi analizować sytuacje w środowisku bezpieczeństwa informacyjnego, określać samodzielnie kierunki rozwoju polityki bezpieczeństwa i precyzować zasadne projekty dla bezpieczeństwa informacyjnego;		+	+		+					+						+	+		+	
EUP_K03	Potrafi analitycznie i rzetelnie ocenić efektywność własnej pracy, pracy zespołu oraz stopień zaangażowania i zaawansowania w zadanie;			+	+				+		+	+	+	+		+	+	+		+	
EUP-K04	Potrafi samodzielnie formułować propozycje i rozwiązania sytuacji problemowych, kryzysowych na podstawie analizy i oceny sytuacji i wydarzeń; potrafi		+		+		+				+			+						+	

Symbol efektów uczenia się dla programu studiów podyplomowych	Efekt uczenia się dla programu studiów podyplomowych		PRZEDMIOTY																	
		Podstawy zarządzania bezpieczeństwem informacji	Zarządzanie ryzykiem	Praktyczne metody zarządzania systemem bezpieczeństwa informacji	Socjotechnika w zarządzaniu bezpieczeństwem informacji	Współczesne zagrożenia dla bezpieczeństwa informacji	Uwarunkowania prawne ochrony informacji	Ochrona informacji w wymiarze narodowym i sojuszniczym	Wybrane problemy kryminalistyki Przestępstwa komputerowe	Prawne aspekty bezpieczeństwa systemów teleinformatycznych	Polityka bezpieczeństwa informacji	Audyt wewnętrzny i zewnętrzny	Tworzenie strategii i polityk bezpieczeństwa informacyjnego	Gra decyzja	Walka, wojna i operacje informacyjne	Oblicza współczesnej propagandy, dezinformacji i manipulacji.	Elementy komunikowania strategicznego w biznesie	Wyostrzanie social mediów w biznesie	Kontrola strategiczna	Seminarium dyplomowe	
	konkretyzować pomysły, myśleć i działać w sposób zgodny z interesami organizacji, podejmować decyzje przedsiębiorcze i pozytywne dla interesu organizacji;																			
EUP_K05	jest gotowa/gotów do postępowania zgodnego z normami etycznymi oraz prawnymi w nauce i działalności zawodowej, w tym do ich propagowania w rolach społecznych i zawodowych;	+	+	+			+	+								+			+	+	