Załącznik
do Uchwały Nr 63/000/2023 Senatu AJP
z dnia 19 grudnia 2023 r.

AKADEMIA IM. JAKUBA Z PARADYŻA W GORZOWIE WIELKOPOLSKIM

PROGRAM STUDIÓW PODYPLOMOWYCH

Nazwa Wydziału prowadzącego studia podyplomowe:	**Wydział Administracji i Bezpieczeństwa Narodowego**	
Nazwa studiów podyplomowych:	**Informatyka śledcza i zwalczanie cyberprzestępczości**	
Poziom studiów:	**studia podyplomowe**	
Forma studiów:	**niestacjonarna**	
Język zajęć:	**język polski**	
Liczba semestrów:	**2**	
Liczba punktów ECTS konieczna do osiągnięcia efektów uczenia się:	**30**	
Umiejscowienie kierunku studiów w dziedzinie/dziedzinach oraz dyscyplinie/dyscyplinach naukowych wraz wskazaniem dyscypliny wiodącej oraz procentowy udział liczby punktów ECTS dla dyscyplin w ogólnej liczbie punktów ECTS wymaganej do ukończenia studiów na kierunku:	**Dziedzina nauk społecznych** w dyscyplinie naukowej:	
	nauki prawne (dyscyplina wiodąca)	**70 %**
	nauki o bezpieczeństwie	**30 %**

1. **Charakterystyka studiów**

Realizacja studiów podyplomowych pn.: *Informatyka śledcza i zwalczanie cyberprzestępczości* została objęta patronatem honorowym Komendanta Wojewódzkiego Policji w Gorzowie Wielkopolskim.

Program studiów podyplomowych pn.: *Informatyka śledcza i zwalczanie cyberprzestępczości* oprócz szerokiego zakresu ramowego, realizuje również program nauczania przewidziany decyzją nr 7 Komendanta Głównego Policji z dnia 15 stycznia 2019 r. *w sprawie programu nauczania na kursie specjalistycznym dla policjantów realizujących zadania w zakresie zwalczania cyberprzestępczości*.

Celem studiów podyplomowych jest uzyskanie wiedzy, umiejętności i kompetencji społecznych przygotowujących absolwentów do realizacji zadań dotyczących zwalczania cyberprzestępczości głównie w zakresie poznania narzędzi prawnych, sposobów, metod i technik pracy oraz analizowania i wyjaśniania spraw w realizacji zadań dotyczących zwalczania cyberprzestępczości; dokonywania oceny zachowania sprawcy cyberprzestępstwa i możliwości jego identyfikacji; przeprowadzenia rozpoznania internetowego, ujawniania i zabezpieczania śladów i dowodów cyfrowych wraz z ich wstępną weryfikacją i dokumentowaniem czynności. Program pozwoli absolwentom na poznanie i zrozumienie różnych procesów i narzędzi informatycznych w zwalczaniu cyberprzestępczości tj. informatyki śledczej, metodyki testów penetracyjnych oraz analizy malware. Ponadto, w trakcie studiów słuchaczom przedstawiona zostanie problematyka i szczegółowa specyfika pracy związanej z Białym wywiadem jak i Cyber Threat Intelligence oraz Wymiarem sprawiedliwości i pomocą prawna w dochodzeniach karnych w cyberprzestrzeni.

Studia podyplomowe dotyczące Zwalczania cyberprzestępczości są przeznaczone głównie dla policjantów służby kryminalnej i śledczej, którzy realizują zadania związane z prowadzeniem spraw w zakresie cyberprzestępczości; policjantów Centralnego Biura Zwalczania Cyberprzestępczości (CBZC); pracowników podmiotów wchodzących w skład Krajowego Systemu Cyberbepieczeństwa; pracowników działów Security Operations Center zajmujących się wykrywaniem, analizowaniem i reagowaniem na incydenty związane z cyberbezpieczeństwem; prawników i absolwentów innych kierunków studiów chcących zdobyć nowe kwalifikacje czy też nową wiedzę, umiejętności i kompetencje w zakresie rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, zapobiegania tym przestępstwom, wykrywania i ścigania sprawców tych przestępstw jak również cyberbezpieczeństwa.

Z uwagi na wysoki poziom merytoryczny oraz przygotowanie i doświadczenie zawodowe osób prowadzących zajęcia z pewnością studia podyplomowe pn.: *Informatyka*

śledcza i zwalczanie cyberprzestępczości będą stanowiły usługę edukacyjną AJP o dużej wartości merytorycznej dla słuchaczy.

2. Wymagania wstępne – konieczne kompetencje kandydatów

Kandydat ubiegający się o przyjęcie na studia podyplomowe pn.: *Informatyka śledcza i zwalczanie cyberprzestępczości* powinien posiadać tytuł magistra, licencjata, inżyniera lub równorzędny, w tym posiadający dyplom uzyskany za granicą zgodnie zasadami określonymi w Zarządzeniu Rektora w sprawie zasad organizowania i dokumentowania studiów podyplomowych w AJP.

3. Cele kształcenia

Kategoria celu kształcenia	Symbol celu kształcenia	Opis celu kształcenia
Wiedza	CSP_W01	Słuchacz zna i rozumie narzędzia prawne zwalczania cyberprzestępczości.
	CSP_W02	Słuchacz posiada pogłębioną wiedzę na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
Umiejętności	CSP_U01	Słuchacz potrafi analizować i wyjaśnić sprawy/stan faktyczny w realizacji zadań dotyczących zwalczania cyberprzestępczości.
	CSP_U02	Słuchacz potrafi dokonać oceny zachowania sprawcy cyberprzestępstwa i możliwości jego identyfikacji.
	CSP_U03	Słuchacz potrafi przeprowadzić ukierunkowane rozpoznanie internetowe oraz dokumentować ww. czynności.
	CSP_U04	Słuchacz potrafi ujawniać i zabezpieczać ślady i dowody cyberprzestępczości wraz z ich wstępną weryfikacją.
Kompetencje	CSP_K01	Słuchacz posiada zdolność krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących zwalczania cyberprzestępczości.
	CSP_K02	Słuchacz postępuje zgodnie ze standardami i regulacjami prawnymi dotyczącymi zwalczania cyberprzestępczości.

4. Efekty uczenia się

Tabela odniesienia efektów uczenia się zdefiniowanych dla programu studiów do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego po uzyskaniu kwalifikacji pełnej na poziomie 4 – poziomy 6-7			
symbol efektów uczenia się dla kierunku	Nazwa efektów uczenia się	Kod składnika opisu z charakterystyk poziomów w PRK po uzyskaniu kwalifikacji pełnej na poziomie 4 – poziomy 6-7	Oznaczenie stosownym symbolem czy efekt odnosi się do charakterystyk uniwersalnych, charakterystyk wspólnych, inżynierskich lub nauczycielskich wraz ze wskazaniem kodu dyscypliny
WIEDZA: absolwent zna i rozumie			

SP_W01	zna i rozumie polskie, europejskie i międzynarodowe narzędzia prawne zwalczania cyberprzestępczości	P7S_WG	U W	V.7
SP_W02	zna i rozumie specyfikę pracy związanej ze zwalczaniem cyberprzestępczości	P7S_WK	U W	V.7
SP_W03	zna i rozumie metody i techniki pracy dotyczącej zwalczania cyberprzestępczości	P7S_WK	U W	V.3 V.7
UMIEJĘTNOŚCI: absolwent potrafi				
SP_U01	potrafi zastosować różne narzędzia np. informatyczne, prawne w zwalczaniu cyberprzestępczości	P7S_UW	U W	V.3 V.7
SP_U02	potrafi dokonać oceny zachowania sprawcy znając możliwości jego identyfikacji również za pomocą różnych środków i narzędzi	P7S_UW	U W	V.7
SP_U03	potrafi ujawniać i zabezpieczać ślady oraz dowody cyberprzestępczości wraz z ich wstępną weryfikacją	P7S_UO	U W	V.3 V.7
SP_U04	potrafi przeprowadzić ukierunkowane rozpoznanie internetowe oraz dokumentować te czynności	P7S_UO	U W	V.3 V.7
KOMPETENCJE SPOŁECZNE: absolwent jest gotów do				
SP_K01	posiada zdolność do krytycznej oceny sytuacji oraz efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących zwalczania cyberprzestępczości	P7S_KK	U W	V.3 V.7
SP_K02	potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości	P7S_KR	U W	V.7

Objaśnienie stosowanych skrótów:

Symbol efektu uczenia się dla kierunku - kolumna 1		
litera SP	dla wyróżnienia, że chodzi o efekty na poziomie studiów podyplomowych	
znak _	podkreślnik	
litera W	dla oznaczenia kategorii efektów – wiedza	
litera U	dla oznaczenia kategorii efektów – umiejętności,	
litera K	dla oznaczenia kategorii efektów – kompetencje społeczne,	
01, 02 i kolejne	numer efektu w obrębie danej kategorii, zapisany w postaci dwóch cyfr (numery należy poprzedzić cyfrą 0)	
Charakterystyki poziomów PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego (drugiego stopnia) - kolumna 3		
P	poziom PRK (6-7)	
S	charakterystyki typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego	
W (wiedza)	**G**	zakres i głębia
	K	kontekst
U (umiejętności)	**W**	wykorzystanie wiedzy
	K	komunikowanie się
	O	organizacja pracy
	U	uczenie się

K (kompetencje społeczne)	**K**	oceny
	O	odpowiedzialność
	R	rola zawodowa
Właściwy kod dyscypliny określony w *Wykazie dziedzin nauki/sztuki i dyscyplin naukowych oraz dyscyplin artystycznych*, stanowiącym załącznik nr 2 do Zarządzenia Nr 81/0101/2018 Rektora AJP z dnia 17 września 2018 r. w sprawie informacji o uprawianej dyscyplinie naukowej, zmienionym Zarządzeniem Nr 60/0101/2020 Rektora AJP z dnia 1 września 2020 r. – kolumna 4		
V.3	nauki o bezpieczeństwie	
V.7	nauki prawne	
Oznaczenia uniwersalne		
U	oznaczenie uniwersalnych charakterystyk pierwszego stopnia Polskiej Ramy Kwalifikacji – poziomy 6-7, o których mowa w pkt 2 – kolumna 4	
W	oznaczenie charakterystyki drugiego stopnia Polskiej Ramy Kwalifikacji – poziomy 6-7 wspólnych dla wszystkich kierunków studiów - kolumna 4	
inż.	oznaczenie kwalifikacji obejmujących kompetencje inżynierskie – kolumna 4	
naucz	oznaczenie kwalifikacji obejmujących kompetencje nauczycielskie – kolumna 4	

5. Plan studiów podyplomowych

L.p.	Nazwa przedmiotu	Liczba godzin	Forma zajęć	Forma zaliczenia	Punkty ECTS
I semestr					
1.	Wstęp do informatyki	10/10	Wykład/ćwiczenia	Zaliczenie z oceną	2
2.	Uregulowania prawne i taktyka prowadzenia wybranych czynności dowodowych	10/10	Wykład/ćwiczenia	Egzamin	2
3.	Działania operacyjne w Internecie	10/10	Wykład/ćwiczenia	Zaliczenie z oceną	2
4.	Podstawy informatyki śledczej cz.1 (ujawnienie i zabezpieczenie materiału dowodowego)	10/10	Wykład/ćwiczenia	Zaliczenie z oceną	2
5.	Analiza śledcza w sprawach związanych z cyberprzestępczością	10/10	Wykład/ćwiczenia	Egzamin	2
6.	Live Forensics, metody TRIAGE	10/10	Wykład/ćwiczenia	Zaliczenie z oceną	2
7.	Seminarium	10	Seminarium	Zaliczenie	3
Łączna liczba zrealizowanych godzin:		**130**	**Łączna liczba punktów ECTS:**		**15**
II semestr					
8.	Podstawy informatyki śledczej cz. 2 - (odzyskiwanie danych i weryfikacja zawartości materiału dowodowego)	8/8	Wykład/ćwiczenia	Egzamin	2
9.	Metodyka testów penetracyjnych z elementami socjotechniki	8/8	Wykład/ćwiczenia	Zaliczenie z oceną	2
10.	Biały wywiad i Cyber Threat Intelligence	8/8	Wykład/ćwiczenia	Zaliczenie z oceną	2
11.	Wprowadzenie do analizy malware	8/8	Wykład/ćwiczenia	Zaliczenie z oceną	2

12.	Wymiar sprawiedliwości i pomoc prawna w dochodzeniach karnych w cyberprzestrzeni	8/8	Wykład/ćwiczenia	Egzamin	2
13.	Seminarium	20	Seminarium	Zaliczenie z oceną pracy pisemnej	5
Łączna liczba zrealizowanych godzin:		**100**	**Łączna liczba punktów ECTS:**		**15**
RAZEM:		**230**	**RAZEM:**		**30**

6. **Przedmioty wraz z przypisaniem do każdego przedmiotu (modułu) zakładanych efektów uczenia się oraz liczby punktów ECTS stanowią załącznik nr 1.**

7. **Wymogi związane z uzyskaniem kwalifikacji podyplomowych.**

Warunkiem wydania świadectwa ukończenia studiów podyplomowych jest osiągnięcie określonych w programie studiów podyplomowych efektów uczenia się, zdobycie wymaganych planem studiów 30 punktów ECTS oraz złożenie pracy końcowej.