



*Załącznik nr 1
do Uchwały Senatu UEK nr T.0022.35.2024
z dnia 29 kwietnia 2024 roku*

PROGRAM STUDIÓW PODYPLOMOWYCH

Cyberbezpieczeństwo w prawie i praktyce

Instytut Prawa UEK, Katedra Prawa Gospodarczego Publicznego i Prawa Pracy

1. Adresaci studiów:

Adresatami studiów są osoby zainteresowane zdobyciem praktycznej wiedzy z zakresu funkcjonowania regulacji prawnych w cyberprzestrzeni oraz zarządzania cyberbezpieczeństwem w organizacjach z sektora publicznego i prywatnego. Studia skierowane są w głównej mierze do przedstawicieli aktualnej i potencjalnej kadry zarządzającej oraz pracowników średniego szczebla w firmach, które aktywnie wykorzystują rozwiązania cyfrowe, chmurowe, a także osób, którym zależy na wdrażaniu wysokiej jakości standardów bezpieczeństwa w organizacjach, które reprezentują.

2. Cel studiów:

Celem studiów jest przekazanie uczestnikom specjalistycznej wiedzy z zakresu prawa cyberprzestrzeni, podstaw systemów informatycznych i technicznych związanych z bezpieczeństwem danych. Ponadto celem studiów – dzięki ich interdyscyplinarności – jest również wykształcenie praktycznych umiejętności zarządzania w obszarze IT, bezpieczeństwem informacji, w tym identyfikacji zagrożeń i przeciwdziałania im. Wiedza i umiejętności pozyskane w czasie studiów pozwolą absolwentowi na specjalizację w ramach swojej pracy w organach ścigania, instytucjach państwowych oraz w biznesie w obszarze związanym z cyberbezpieczeństwem. Studia mają charakter interdyscyplinarny, zajęcia prowadzone są głównie przez praktyków - prawników, informatyków, ekonomistów.

3. Program studiów:

MODUŁ	NAZWA PRZEDMIOTU	LICZBA GODZIN	PUNKTY ECTS
1.	Cyberbezpieczeństwo jako nowy obszar bezpieczeństwa – ujęcie definicyjne	10	2
2.	Zarządzanie informacją	10	2
3.	Prawne aspekty nowych technologii	10	2
4.	Prawne aspekty ochrony danych osobowych	20	3
5.	Cyberprzestępczość w prawie własności intelektualnej	20	3
6.	Umowy w cyberprzestrzeni	15	3
7.	Zabezpieczenie dowodów w postępowaniu cywilnym	8	1
8.	Cyberprzestępczość w prawie karnym	8	1
9.	Cyberbezpieczeństwo sektorowe. Wybrane zagadnienia i problemy	9	1
10.	Wstęp do informatyki z elementami programowania	30	3
11.	Wymagania normy ISO 27001	8	3
12.	Audytywanie normy ISO 27001	16	3
13.	Zarządzanie bezpieczeństwem informacji w praktyce	16	3
	Razem	180	30

4. Czas trwania studiów oraz liczba godzin:

Studia podyplomowe odbywać będą się w trybie niestacjonarnym (w piątki, soboty, w wyjątkowych sytuacjach w niedziele). Wymiar godzin studiów podyplomowych to 180. Czas trwania studiów podyplomowych to dwa semestry.

5. Warunki oraz sposób zaliczenia studiów:

Warunkiem uzyskania zaliczenia każdego przedmiotu jest obecność na zajęciach. Osoby nieobecne z przyczyn losowych będą indywidualnie ustalać warunki zaliczenia przedmiotu. Każdy semestr kończy się egzaminem w formie testowej, obejmującym zagadnienia omawiane na wszystkich przedmiotach w danym semestrze. Warunkiem ukończenia studiów jest uzyskanie pozytywnego wyniku z egzaminu końcowego, w formie testu jednokrotnego wyboru.

6. Efekty uczenia się:

Efekty uczenia się dla studiów podyplomowych		
Jednostka prowadząca:	Krakowska Szkoła Biznesu UEK	
Nazwa studiów podyplomowych:	<i>Cyberbezpieczeństwo w prawie i praktyce</i>	
Dziedzina nauki:	Nauki społeczne	
Profil studiów:	ogólnoakademicki	
Poziom PRK	7	
Poziom studiów:	podyplomowe	
Liczba semestrów:	2	
Symbol efektu uczenia się dla kierunku	Opis efektów uczenia się	Odniesienie do charakterystyk efektów uczenia się
P_W (WIEDZA) Absolwent zna i rozumie:		
CPP_W1	w pogłębionym stopniu teorie i koncepcje oraz zależności ekonomiczno-społeczne, stanowiące zaawansowaną wiedzę z zakresu zarządzania bezpieczeństwem cyfrowym, zarówno w organizacjach publicznych, jak i niepublicznych.	P7S_WG
CPP_W2	w pogłębionym stopniu teorie wyjaśniające złożoność funkcjonowania podmiotów związanych z obszarem szeroko rozumianego zarządzania, zarówno w odniesieniu do poziomu operacyjnego, jak i menedżerskiego podmiotów wykorzystujących zaawansowane technologicznie rozwiązania cyfrowe.	P7S_WG
CPP_W3	w pogłębionym stopniu proces zmian zachodzący w obszarze zarządzania i bezpieczeństwa internetowego, nie tylko w kontekście ich przyczyn, przebiegu i konsekwencji, a także uwarunkowań etycznych i cywilizacyjnych.	P7S_WG
CPP_W4	w pogłębionym stopniu prawne, organizacyjne i etyczne uwarunkowania wykonywania działalności zawodowej w obszarze zarządzania bezpieczeństwem cyfrowym.	P7S_WK
CPP_W5	w pogłębionym stopniu zasady ochrony własności intelektualnej i prawa autorskiego w kontekście ogólnym oraz z dziedziny nauk społecznych i prawnych.	P7S_WK
P_U (UMIEJĘTNOŚCI) Absolwent potrafi:		
CPP_U1	wykorzystać posiadaną wiedzę do twórczego formułowania i rozwiązywania złożonych oraz niestandardowych problemów, związanych z zarządzaniem bezpieczeństwem informatycznym,	P7S_UW

	kontrolą oraz wdrażaniem innowacyjnych i kreatywnych rozwiązań, a także właściwie dobierać źródła informacji i dokonywać ich weryfikacji.	
CPP_U2	prawidłowo interpretować i wyjaśniać zjawiska oraz procesy w odniesieniu do zagadnień związanych z prawnymi aspektami bezpieczeństwa cyfrowego.	P7S_UW
CPP_U3	dobierać i stosować właściwe metody i narzędzia, w tym zaawansowane techniki informacyjno – komunikacyjne oraz informatyczne, a także fachowe słownictwo do rozwiązywania pojawiających się problemów w zakresie prawnych i zarządczych aspektów bezpieczeństwa cyfrowego organizacji.	P7S_UW
CPP_U4	komunikować się na tematy związane z cyberbezpieczeństwem z szerokim i zróżnicowanym kręgiem odbiorców i partnerów.	P7S_UK
CPP_U5	kierować pracą zespołu, współdziałać z innymi osobami w ramach prac zespołowych, przyjmując postawę lidera, motywować i inspirować członków zespołu do aktywności.	P7S_UO
CPP_U6	samodzielnie planować i realizować własne uczenie się przez całe życie oraz ukierunkowywać innych w tym zakresie.	P7S_UU
P_K (KOMPETENCJE SPOŁECZNE) Absolwent jest gotów do:		
CPP_K1	uznawania znaczenia wiedzy w rozwiązywaniu problemów zarządczych i praktycznych dotyczących kontroli oraz sygnalizowania nieprawidłowości dot. cyberbezpieczeństwa.	P7S_KK
CPP_K2	korzystania z opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów zarządczych i kontrolnych.	P7S_KK
CPP_K3	wypełniania zobowiązań społecznych oraz inspirowania i organizowania działalności na rzecz środowiska społecznego.	P7S_KO
CPP_K4	inicjowania działania na rzecz interesu publicznego w tym w obszarze cyberbezpieczeństwa.	P7S_KO
CPP_K5	myślenia i działania w sposób przedsiębiorczy	P7S_KO
CPP_K6	odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, w tym do podtrzymywania odpowiedniego etosu zawodu.	P7S_KR

Objaśnienia oznaczeń w symbolach dotyczących kierunku studiów podyplomowych:

CPP – kierunek studiów podyplomowych Cyberbezpieczeństwo w prawie i praktyce.

W – kategoria wiedzy

☐ U – kategoria umiejętności

☐ K – kategoria kompetencji społecznych

☐ 1, 2, 3 i kolejne – numer efektu uczenia się



Objaśnienia oznaczeń w odniesieniach do charakterystyk efektów uczenia się

- ☐ P – poziom Polskiej Ramy Kwalifikacji (PRK)
- ☐ P7S – charakterystyka drugiego stopnia poziomu 7 PRK

P7U_W – charakterystyka uniwersalna (WIEDZA):

- ☐ P7S_WG – charakterystyka drugiego stopnia (zakres i głębia)
- ☐ P7S_WK – charakterystyka drugiego stopnia (kontekst)

P7U_U – charakterystyka uniwersalna (UMIEJĘTNOŚCI):

- ☐ P7S_UW – charakterystyka drugiego stopnia (wykorzystanie wiedzy)
- ☐ P7S_UK – charakterystyka drugiego stopnia (komunikowanie się)
- ☐ P7S_UO – charakterystyka drugiego stopnia (organizacja pracy)
- ☐ P7S_UU – charakterystyka drugiego stopnia (uczenie się)

P7U_K – charakterystyka uniwersalna (KOMPETENCJE SPOŁECZNE):

- ☐ P7S_KK – charakterystyka drugiego stopnia (oceny/krytyczne podejście)
- ☐ P7S_KO – charakterystyka drugiego stopnia (odpowiedzialność)
- ☐ P7S_KR – charakterystyka drugiego stopnia (rola zawodowa)