Załącznik nr 1
do Uchwały Senatu UEK nr T.0022.17.2022
z dnia 25 kwietnia 2022 roku

PROGRAM STUDIÓW PODYPLOMOWYCH

Cyberbezpieczeństwo – aspekty prawne i praktyczne

prowadzonych wspólnie z Katedrą 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 systemami 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.

3. Program studiów:

L.p.	Przedmiot	Wymiar godzinowy	ECTS
MODUŁ I	**Cyberbezpieczeństwo – aspekty prawne i organizacyjne**	**88**	**15**
1.	Wprowadzenie do prawa nowych technologii	16	3
2.	Cyberbezpieczeństwo w prawie UE	12	2
3.	Prawo własności intelektualnej w cyberprzestrzeni **	12	2
4.	Ochrona danych osobowych	12	2
5.	Umowy w cyberprzestrzeni	12	2
6.	Cyberbezpieczeństwo w administracji publicznej	12	2
7.	Psychologiczne aspekty cyberbezpieczeństwa**	12	2
MODUŁ II	**Cyberbezpieczeństwo w praktyce**	**92**	**15**
8.	Wprowadzenie do cyberbezpieczeństwa	12	2
9.	Rozwiązania techniczne w cyberbezpieczeństwie	12	2
10.	Bezpieczeństwo baz danych, aplikacji www i urządzeń mobilnych	12	2
11.	Bezpieczeństwo systemów i sieci komputerowych	12	2
12.	Bezpieczeństwo infrastruktury sieciowej	12	2
13.	Elementy informatyki	12	2

14.	AI, Big Data, 5G i inne wyzwania dla cyberprzestrzeni	12	2
15.	Kurs do wyboru/Kurs online*	8	1
	Razem	**180**	**30**

** szkolenie certyfikowane * tematyka kursu dobrana zgodnie z sugestią grupy lub przedmiot z dostępnych w ofercie Krakowskiej Szkoły Biznesu.

4. Czas trwania studiów oraz liczba godzin:

Studia podyplomowe odbywać będą się w trybie niestacjonarnym (dwa razy w miesiącu w piątki, soboty lub 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. Każdy semestr kończy się egzaminem w formie testowej, obejmującym zagadnienia omawiane na wszystkich przedmiotach w danym semestrze. Warunkiem ukończenia studiów jest przystąpienie do egzaminu końcowego.

6. Efekty uczenia się:

Efekty uczenia się dla studiów podyplomowych		
Jednostka prowadząca:	Krakowska Szkoła Biznesu UEK	
Nazwa studiów podyplomowych:	***Cyberbezpieczeństwo – aspekty prawne i praktyczne***	
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:		
CAPP_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	**P7S_WG**

	niepublicznych.	
CAPP_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**
CAPP_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_WK**
CAPP_W4	w pogłębionym stopniu prawne, organizacyjne i etyczne uwarunkowania wykonywania działalności zawodowej w obszarze zarządzania bezpieczeństwem cyfrowym.	**P7S_WK**
CAPP_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:		
CAPP_U1	wykorzystać posiadaną wiedzę do twórczego formułowania i rozwiązywania złożonych oraz niestandardowych problemów, związanych z zarządzaniem bezpieczeństwem informatycznym, kontrolą oraz wdrażaniem innowacyjnych i kreatywnych rozwiązań, a także właściwie dobierać źródła informacji i dokonywać ich weryfikacji.	**P7S_UW**
CAPP_U2	prawidłowo interpretować i wyjaśniać zjawiska oraz procesy w odniesieniu do zagadnień związanych z prawnymi aspektami bezpieczeństwa cyfrowego.	**P7S_UW**
CAPP_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**
CAPP_U4	komunikować się na tematy związane z cyberbezpieczeństwem z szerokim i zróżnicowanym kręgiem odbiorców i partnerów.	**P7S_UK**

CAPP_U5	kierować pracą zespołu, współdziałać z innymi osobami w ramach prac zespołowych, przyjmując postawę lidera, motywować i inspirować członków zespołu do aktywności.	**P7S_UO**
CAPP_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:		
CAPP_K1	uznawać znaczenie wiedzy w rozwiązywaniu problemów zarządczych i praktycznych dotyczących kontroli oraz sygnalizowania nieprawidłowości.	**P7S_KK**
CAPP_K2	korzystać z opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemów zarządczych i kontrolnych.	**P7S_KK**
CAPP_K3	do wypełniania zobowiązań społecznych oraz inspirowania i organizowania działalności na rzecz środowiska społecznego.	**P7S_KO**
CAPP_K4	inicjować działania na rzecz interesu publicznego w tym w obszarze cyberbezpieczeństwa.	**P7S_KO**
CAPP_K5	do myślenia i działania w sposób przedsiębiorczy.	**P7S_KO**
CAPP_K6	do 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:

CAPP– kierunek studiów podyplomowych ***Cyberbezpieczeństwo – aspekty prawne i praktyczne***

- **W** – kategoria wiedzy
- **U** – kategoria umiejętności
- **K** – kategoria kompetencji społecznych
- **01, 02, 03 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)