Możliwość dofinansowania

Cyberbezpieczeństwo w prawie i praktyce 2024/2025.

Numer usługi 2024/05/14/8419/2149299

6 000,00 PLN brutto
6 000,00 PLN netto
33,33 PLN brutto/h
33,33 PLN netto/h

Uniwersytet Ekonomiczny w Krakowie

★★★★½

Kraków / stacjonarna
Studia podyplomowe
180 h
01.10.2024 do 31.07.2025

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo pozostałe
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Ten kierunek jest dla Ciebie, jeżeli: >jesteś zainteresowana/y zdobyciem praktycznej wiedzy z zakresu regulacji prawnych w cyberprzestrzeni i zarządzania cyberbepzpieczeństwem, >chcesz zdobyć uprawnienia do pracy na stanowisku Audytora wiodącego/wewnętrznego systemów zarządzania Bezpieczeństwem Informacyjnym (Audytor wiodący ISO 27001 lub Audytor wewnętrzny ISO 27001), >zależy Ci na wdrażaniu wysokiej jakości standardów bezpieczeństwa w Twojej organizacji, >aktywnie wykorzystujesz rozwiązania cyfrowe i chmurowe.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	15-09-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	180
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)

Zakres uprawnień	Studia podyplomowe

Cel

Cel edukacyjny

Studia Cyberbezpieczeństwo w prawie i praktyce 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.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisane pod Programem	Egzamin	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Świadectwo

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Egzamin

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

ECTS

Program

LP	Nazwa Przedmiotu	Godziny	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	Audytowanie normy ISO 27001	16	3
13	Zarządzanie bezpieczeństwem informacji w praktyce	16	3
	RAZEM:	180	30

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)

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.				

Cennik

Cennik

Rodzaj ceny	Cena
Koszt usługi brutto	6 000,00 PLN
Koszt usługi netto	6 000,00 PLN
Koszt godziny brutto	33,33 PLN
Koszt godziny netto	33,33 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

dr hab. Monika Szaraniec, prof. UEK

Wykładowca na programie Cyberbezpieczeństwo w prawie i praktyce.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały załączone w systemie LMS (system wenętrzny KSB UEK).

Warunki uczestnictwa

Posiadanie wykształcenia wyższego.

Informacje dodatkowe

Szczegółowe informacje o kierunku znajdują się na stronie: www.ksb.uek.krakow.pl

Adres

ul. Rakowicka 27
31-510 Kraków

woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Łukasz Kos

E-mail lukasz.kos@uek.krakow.pl
Telefon (+48) 12 2937 596