WYDZIAŁ PRAWA, ADMINISTRACJI I EKONOMII
DZIEKANAT
Ul. Uniwersytecka 22/26
50 – 145 Wrocław

Tel. +48 713752371
Tel. +48 691944003
podyplomowe.wpae@uwr.edu.pl / podyplomowe.prawo.uni.wroc.pl

Wrocław, dnia 16 marca 2023 r.

Wydział Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego
ogłasza zapisy na
Studia Podyplomowe

Zarządzanie Cyberbezpieczeństwem w praktyce

w roku akademickim 2023/2024

Nazwa studiów podyplomowych, w tym nazwa studiów w tłumaczeniu na język angielski: Studia podyplomowe Zarządzanie Cyberbezpieczeństwem w praktyce/ Cybersecurity Management

Kierownik studiów podyplomowych: dr Piotr Ochman

Kwalifikacje uzyskane po ukończeniu studiów: kwalifikacje cząstkowe na poziomie 7. Absolwent otrzymuje świadectwo ukończenia studiów podyplomowych

Forma prowadzenia studiów: Dwusemestralne studia podyplomowe w trybie niestacjonarnym (zjazdy: sobota i niedziela)

W roku akademickim 2023/2024 zajęcia będą prowadzone zdalnie - aplikacja MS Teams.

Profil studiów: Studia mają na celu wyposażenie słuchaczy w wiedzę, umiejętności i kompetencje z zakresu teoretycznych i praktycznych zagadnień związanych z wykonywaniem zadań w zakresie zarządzania cyberbezpieczeństwem. Atutem studiów jest połączenie zagadnień z zakresu prawa i informatyki z problematyką ekonomiczną, psychologiczną, a także z zakresu zarządzania.

Adresat studiów: Studia są przeznaczone dla praktyków prawa, administracji, zarządzania, a także osób odpowiedzialnych za bezpieczeństwo w organizacjach, którzy chcą uzyskać odpowiednią wiedzę, umiejętności i doświadczenie w zakresie skomplikowanej i interdyscyplinarnej problematyki zarządzania cyberbezpieczeństwem w organizacji.

Wymagania wstępne dla kandydatów, zasady rekrutacji: Zgodnie z Regulaminem studiów podyplomowych (Uchwała Nr 154/2019 Senatu Uniwersytetu Wrocławskiego z dnia 20 listopada 2019 r. w sprawie regulaminu studiów podyplomowych w Uniwersytecie Wrocławskiem wraz z późniejszymi zmianami), na studia podyplomowe może być przyjęta

osoba, która posiada kwalifikację pełną co najmniej na poziomie 6 PRK uzyskaną w systemie szkolnictwa wyższego i nauki.

Kandydaci na studia podyplomowe powinni złożyć w Dziekanacie następujące dokumenty:

a. podanie o przyjęcie na studia podyplomowe wydrukowane z systemu IRK i podpisane przez kandydata wraz z oświadczeniem o zapoznaniu się z treścią wzoru umowy (czyli: formularz rejestracyjny ON-LINE zamieszczony na stronie www.irka.uni.wroc.pl),

b. kserokopię dyplomu wraz z oryginałem do wglądu lub poświadczony notarialnie dyplom.

Zasady odpłatności: 11.499,00 zł (jedenaście tysięcy czterysta dziewięćdziesiąt dziewięć złotych) za dwa semestry, płatne zgodnie z postanowieniami umowy o świadczeniu usług edukacyjnych; nie jest przewidziana opłata rekrutacyjna.

Kwalifikacje uzyskane po ukończeniu studiów: Kwalifikacje cząstkowe na poziomie 7. Absolwent otrzymuje świadectwo ukończenia studiów podyplomowych, a także certyfikat Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001, certyfikat Pełnomocnika ds. cyberbezpieczeństwa świadczonych usług kluczowych zgodnych z ISO 27001, ISO 22301 oraz RODO oraz zaświadczenie o ukończeniu szkolenia Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 wystawione przez DEKRA Polska sp. z o.o.

Opis kadry dydaktycznej: Prowadzącymi zajęcia są praktycy oraz nauczyciele akademiccy. Praktykami prowadzącymi zajęcia są m. in. radcowie prawni oraz adwokaci, sędziowie, prokuratorzy, specjaliści w zakresie cyberbezpieczeństwa. Praktycy prowadzący zajęcia wykazują się wieloletnim doświadczeniem zawodowym odpowiadającym tematyce prowadzonych przedmiotów. Nauczyciele akademiccy prowadzący zajęcia są zatrudnieniu na Uniwersytecie Wrocławskim i zajmują się problematyką zawartą w programie studiów.

Program Studiów Podyplomowych
Zarządzanie Cyberbezpieczeństwem w praktyce

Program zajęć trwa 2 semestry i zakłada 226 godz. Zajęć (I semestr – 112 godz., II semestr – 114 godz.)
Łączna liczba punktów ECTS – 74.
Po uzyskaniu wszystkich zaliczeń słuchacze przystępują do egzaminu końcowego.

Lp.	Przedmiot wg programu	Forma zajęć	liczba godz.	Forma zaliczenia	Pkt ECTS	PROWADZĄCY ZAJĘCIA
I semestr						
1	Wprowadzenie do cyberbezpieczeństwa i zarządzania operacyjnego w organizacji	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki

2	Rola i zadania osób odpowiedzialnych za bezpieczeństwo (*Chief Security Officer*, *Chief Information Officer* i *Chief Information Security Officer*)	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
3	Zarządzanie strategiczne cyberbezpieczeństwem	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
4	Architektura cyberbezpieczeństwa	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
5	Aspekty operacyjne cyberbezpieczeństwa (zapobieganie, wykrywanie, odpowiedź)	warsztaty	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
6	Zarządzanie operacyjne 1. Zarządzanie kontrolą dostępu 2, 2. Zarządzanie podatnościami i zagrożeniami (MITRE ATT&CK, Red Team, Purple Team, Blue Team, ewolucja zagrożeń, social engineering, ransomware) 6, 3. Zarządzanie incydentami 4, 4. Zarządzanie bezpieczeństwem aplikacji i danych 2, 5. Zarządzanie bezpieczeństwem sieci 2, 6. Zarządzanie bezpieczeństwem fizycznym 2, 7. Zarządzanie bezpieczeństwem łańcucha dostaw (biały wywiad i weryfikacja kontrahentów (OSiNT)) 4, 8. Zarządzanie zespołem w organizacji 4	warsztaty	26	zaliczenie (zal)	8	praktyk, nauczyciel akademicki
7	Zarządzanie inwestycjami w cyberbezpieczeństwo	wykład	8	zaliczenie (zal)	3	praktyk, nauczyciel akademicki
8	Ubezpieczenia ryzyk cyber	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
9	Współpraca z doradcami zewnętrznymi	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
10	Kluczowe wskaźniki efektywności (KPI) a zarządzanie cyberbezpieczeństwem	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
11	Wprowadzenie do informatyki śledczej	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
12	Stres w miejscu pracy i radzenie sobie z nim	warsztaty	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
13	Wprowadzenie do sieci komputerowych	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
14	Inżynieria systemowa	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
15	Chmura obliczeniowa (cloud computing) i usługi w chmurze	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki

16	Bezpieczeństwo wiodących systemów operacyjnych i aplikacji www	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
17	Urządzenia mobilne	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
18	Internet rzeczy (IoT)	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
19	Praca zdalna	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
20	Praktyczne aspekty informatyki i prawa	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
21	Organy korporacji i organizacja ich funkcjonowania	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
22	Współpraca z organami nadzorczymi oraz organami ścigania i wymiaru sprawiedliwości	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
23	Procedury na wypadek kontroli organów państwowych	warsztaty	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
24	Zgłaszanie nieprawidłowości (sygnaliści)	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
25	Ryzyka regulacyjne w obszarze nowych technologii	warsztaty	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
26	Standaryzacja i certyfikacja w zakresie cyberbezpieczeństwa (ISO 27000, ISO 22301, ISO 27036, standardy NISO, CSF, Polskie Normy). Część I	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
27	Seminarium dyplomowe	seminarium	8	zaliczenie (zal)	3	praktyk, nauczyciel akademicki
razem I semestr			**112**		**38**	
II semestr						
1	Krajowy system cyberbezpieczeństwa	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
2	Cyberbezpieczeństwo a systemy compliance	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
3	Ochrona informacji poufnych i tajemnicy zawodowej	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
4	Ochrona danych osobowych	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
5	Ochrona informacji niejawnych. Bezpieczeństwo teleinformatyczne	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
6	Audytor wiodący systemu zarządzania bezpieczeństwem informacji	wykład	12	zaliczenie (zal)	4	praktyk, nauczyciel akademicki
7	Standaryzacja i certyfikacja w zakresie cyberbezpieczeństwa (ISO 27000, ISO 22301, ISO 27036, standardy NISO, CSF, Polskie Normy). Część II.	warsztaty	8	zaliczenie (zal)	3	praktyk, nauczyciel akademicki
8	System zarządzania bezpieczeństwem informacji	wykład	8	zaliczenie (zal)	3	praktyk, nauczyciel akademicki

9	Cyberbezpieczeństwo usług kluczowych	wykład	12	zaliczenie (zal)	3	praktyk, nauczyciel akademicki
10	Cyberprzestępczość	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
11	Cyberterroryzm	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
12	Wybrane aspekty z zakresu zamówień publicznych	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
13	Opracowywanie procedur wewnętrznych	warsztaty	4	zaliczenie (zal)	2	praktyk, nauczyciel akademicki
14	Pełnomocnik ds. cyberbezpieczeństwa	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
15	Podstawy kryptografii i podpisy cyfrowe	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
16	Shadow IT	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
17	Systemy automatyki przemysłowej	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
18	Blockchain i kryptowaluty	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
19	Sztuczna inteligencja	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
20	Bankowość elektroniczna	wykład	2	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
21	Wojna informacyjna i hybrydowa	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
22	Nowe zagrożenia w zakresie cyberbezpieczeństwa	wykład	4	zaliczenie (zal)	1	praktyk, nauczyciel akademicki
23	Seminarium dyplomowe	seminarium	8	zaliczenie (zal)	3	praktyk, nauczyciel akademicki
razem II semestr			**114**		**35**	

OPIS ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ DLA STUDIÓW PODYPLOMOWYCH ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM W PRAKTYCE

Wydział: Prawa, Administracji i Ekonomii

Studia podyplomowe Zarządzanie cyberbezpieczeństwem w praktyce

Poziom kwalifikacji cząstkowej: 7

Kod efektu uczenia się dla studiów podyplomowych	**Efekty uczenia się**	Odniesienie do charakterystyk drugiego stopnia PRK
	WIEDZA	
SP_W01	Ma pogłębioną wiedzę o miejscu i specyfice zarządzania cyberbezpieczeństwem w otoczeniu gospodarczym, z uwzględnieniem regulacji prawnych, standaryzacji procesów zarządzania zgodnością, w tym zwłaszcza odpowiednich norm branżowych	P7S_WG
SP_W02	Rozumie istotę i funkcje zarządzania cyberbezpieczeństwem w praktyce organizacji	P7S_WG

SP_W03	Zna w pogłębionym stopniu instytucje funkcjonujące w zakresie zarządzania cyberbezpieczeństwem, a także ich zastosowanie do realizacji celów biznesowych zgodnych z przepisami prawa, kodeksami branżowymi, procedurami i regulacjami wewnętrznymi oraz zasadami etyki	P7S_WG
SP_W04	Zna zasady funkcjonowania oraz rolę osób odpowiedzialnych za cyberbezpieczeństwo oraz auditora wewnętrznego	P7S_WK
SP_W05	Zna wymagania regulacyjne i etyczne w zakresie funkcjonowania cyberbezpieczeństwa w organizacji	P7S_WG
UMIEJĘTNOŚCI		
SP_U01	Formułuje złożone pisemne oraz ustne wypowiedzi w zakresie audytu wewnętrznego, uwzględniające relacje z otoczeniem prawnym i regulacyjnym, jak również potrafi dostosować działania firmy do wymogów cyberbezpieczeństwa	P7S_UW
SP_U02	Identyfikuje złożone problemy w zakresie cyberbezpieczeństwa oraz rozwiązuje je posługując się właściwym instrumentarium, w tym prawnym, jak również potrafi projektować systemy zarządzania ryzykiem	P7S_UW
SP_U03	Potrafi opracować procedury cyberbezpieczeństwa i audit wewnętrzny oraz wdrożyć oraz monitorować mechanizmy oraz programy polegające na zapobieganiu i przeciwdziałaniu ryzykom cyber w organizacji	P7S_UK
SP_U04	Dostrzega konsekwencje zastosowania określonych regulacji prawnych w danym stanie faktycznym projektując procedury w zakresie cyberbezpieczeństwa oraz przeprowadzając audit wewnętrzny	P7S_UO
SP_U05	Posiada w pogłębionym stopniu umiejętności interpersonalne w zakresie rozwiązywania problemów z zakresu cyberbezpieczeństwa lub przeprowadzania auditu wewnętrznego	P7S_UU
SP_U06	Sprawnie posługuje się przepisami prawa w codziennej praktyce zawodowej z zakresu cyberbezpieczeństwa oraz potrafi monitorować system zarządzania cyberbezpieczeństwem	P7S_UW
KOMPETENCJE SPOŁECZNE		
SP_K01	Dostrzega konieczność ciągłego doskonalenia i aktualizacji wiedzy z zakresu cyberbezpieczeństwa	P7S_KK

SP_K02	Jest gotów podjęcia pracy jako Chief Security Officer, Chief Information Officer, Chief Information Security Officer, auditor wewnętrzny, specjalista ds. zarządzania cybezbezpieczeństwem, jak również pracownik działu audytu, kontroli wewnętrznej, bezpieczeństwa, zarządzania ryzykiem	P7S_KO
SP_K03	Podkreśla znaczenie rozwoju wiedzy o cyberbezpieczeństwie oraz zastosowaniu jego instytucji w kontekście zmian gospodarczych i społecznych	P7S_KR

Objaśnienie symboli:

PRK – Polska Rama Kwalifikacji

P6S_WG/P7S _WG – kod składnika opisu kwalifikacji dla poziomu 6 i 7 w charakterystykach drugiego stopnia Polskiej Ramy Kwalifikacji

SP_W - kierunkowe efekty uczenia się w zakresie wiedzy

SP_U - kierunkowe efekty uczenia się w zakresie umiejętności

SP_K - kierunkowe efekty uczenia się w zakresie kompetencji społecznych

01, 02, 03 i kolejne - kolejny numer kierunkowego efektu uczenia się