

Część II.A. Informacje o studiach podyplomowych

CYBERBEZPIECZEŃSTWO

.....
(nazwa studiów podyplomowych)

1. Ogólna charakterystyka studiów podyplomowych

1.1 Ogólne cele kształcenia oraz kwalifikacje uzyskiwane przez absolwentów (jeśli ukończenie studiów prowadzi do uzyskania określonych kwalifikacji)

Zapotrzebowanie rynku zdominowanego przez postępującą cyfryzację wszelkich aspektów funkcjonowania społeczeństwa oraz wzrost liczby przestępstw popełnianych względem i przy użyciu cyfrowych urządzeń powoduje, że cyberbezpieczeństwo to dziedzina interdyscyplinarna potrzebująca specjalistów zarówno technicznych, ale również na płaszczyźnie zarządczej.

Celem studiów jest przekazanie praktycznej wiedzy w zakresie cyberbezpieczeństwa w kontekście obszaru technicznego, prawnego i zarządczego. Celem studiów jest zdobycie wiedzy i praktycznych umiejętności z zakresu szeroko rozumianego zarządzania cyberbezpieczeństwem: opracowywania strategii cyberbezpieczeństwa, wdrażania procedur bezpieczeństwa, zarządzania ciągłością działania, incydentami cyberbezpieczeństwa oraz ryzykiem. Przekazywana wiedza uwzględnienia zarówno aspekty zapewnienia ochrony infrastruktury teleinformatycznej i systemów, jak i informacji.

1.2 Wymagania wstępne (oczekiwane kompetencje kandydata)

Studia są adresowane do absolwentów studiów I stopnia, II stopnia lub jednolitych studiów magisterskich, którzy są zainteresowanych zagadnieniami związanymi z cyberbezpieczeństwem i cyberprzestępczością. Studia podyplomowe kierowane są do osób, które zajmują się, bądź planują pracę na stanowiskach związanych z prowadzeniem, planowaniem, kontrolowaniem bezpieczeństwa informacji i systemów, w których dane o różnym stopniu poufności są tworzeniem, przesyłane, przetwarzane albo przechowywane. Ponadto adresatami studiów podyplomowych mogą być administratorzy systemów teleinformatycznych, którzy planują pogłębić swoją wiedzę w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji. Studia podyplomowe cyberbezpieczeństwo dedykowane są: pracownikom administracji publicznej, organów ścigania, wymiaru sprawiedliwości, pracowników sektora bankowego i finansowego oraz pracownikom przedsiębiorstw, które zajmują się działaniami w obszarze cyberbezpieczeństwa. Odbiorcą oferty może być również kadra kierownicza i zarządzająca odpowiedzialna za bezpieczeństwo informacji. Ponadto studia kierowane są do pracowników komórek zarządzania

bezpieczeństwem (Security Operations Center, SOC), jak również ekspertów działów IT, audytorów i pentesterów.

1.3 Zasady rekrutacji

Kandydaci na studia zobowiązani są do elektronicznej rejestracji, a następnie złożenia wymaganych dokumentów. Rekrutacja odbywa się na podstawie kolejności zgłoszeń, do wyczerpania limitu miejsc. Warunkiem uruchomienia studiów jest uzyskanie deklaracji uczestnictwa przez minimum 15 osób.

Wymagane dokumenty:

- elektroniczna rejestracja: <https://webapps.uz.zgora.pl/rekrutacja/>,
- odpis / kopia dyplomu,
- dowód wpłaty opłaty rekrutacyjnej,
- zobowiązanie do ponoszenia kosztów odpłatności za studia.

Decyzję o przyjęciu na studia podyplomowe podejmuje Komisja Rekrutacyjna działająca pod przewodnictwem kierownika studiów podyplomowych. Decyzja o przyjęciu na studia przesyłana jest kandydatowi w formie pisemnej lub elektronicznej.

Limit miejsc: 30.

2. Opis zakładanych efektów kształcenia

Symbol efektu	Efekty uczenia się dla studiów podyplomowych: <i>cyberbezpieczeństwo</i>
WIEDZA W zakresie wiedzy absolwent zna i rozumie:	
W_01	Zna zasady stosowania kryptografii na potrzeby zapewnienia cyberbezpieczeństwa, zna typy ataków cybernetycznych oraz stosuje skuteczne metody przeciwdziałania wybranym rodzajom ataków cybernetycznych również z wykorzystaniem modułów sprzętowych
W_02	Potrafi wskazać kluczowe aspekty budowania architektury systemów teleinformatycznych i cyberbezpiecznych. Zna i potrafi wyjaśnić rodzajów cyberataków, którym mogą zostać poddane infrastruktura, systemy teleinformatyczne i cyberfizyczne oraz wskazać skuteczne metody ochrony przed cyberatakami, również z wykorzystaniem modułów sprzętowych.
W_03	Zna kluczowe aspekty uregulowań prawnych w sektorze IT na potrzeby realizacji wybranych rodzajów testów oraz zakres odpowiedzialności firmy świadczącej usługi Security Operations Center w monitorowaniu cyberbezpieczeństwa klientów. Zna dobre praktyki w zakresie tworzenia regulaminów, polityk prywatności i polityk cookies.
W_04	Zna podstawowe zagadnienia związane z informatyką śledczą w aspekcie zarządzania operacjami bezpieczeństwa oraz zabezpieczania cyfrowego materiału dowodowego
W_05	Zna i potrafi wymienić aspekty zapewnienia bezpieczeństwa sieci, chmury, komputerów osobistych i urządzeń mobilnych oraz bezpieczeństwa fizycznego

	systemów cybernetycznych. Potrafi przygotować plan ciągłości działania.
W_06	Zna i potrafi wyjaśnić rodzaje i etapy realizacji testów penetracyjnych oraz scharakteryzować proces audytu bezpieczeństwa z wykorzystaniem testów penetracyjnych
W_07	Potrafi wskazać i opisać zadania Security Operation Center oraz wymienić technologie i procedury stosowane w celu wykrywania, analizowania, raportowania i reagowania na incydenty związane z cyberbezpieczeństwem oraz zapobiegania tym incydentom
W_08	Zna standardy bezpieczeństwa informacji oraz zasady realizacji audytów bezpieczeństwa teleinformatycznego, oceny i zarządzania ryzykiem oraz metodami, standardami testowania. Zna zasady oceny skuteczności Systemu Zarządzania Bezpieczeństwem Informacji i potrafi przygotować program audytu, a także dokonać analizy jego wyników w kontekście ewentualnego wpływu na bezpieczeństwo przetwarzanych informacji.
W_09	Zna i potrafi scharakteryzować proces analizy, oceny systemów informatycznych, identyfikować zagrożenia dla bezpieczeństwa w cyberprzestrzeni oraz zarządzać ryzykiem w aspekcie Cyber Threat Intelligence
W_10	Potrafi wskazać i scharakteryzować wymagania w zakresie ochrony danych osobowych oraz ochrony informacji niejawnych. Potrafi tworzyć system ochrony informacji osobowych. Ma podstawową wiedzę dotyczącą standardów i norm oraz krajowych i międzynarodowych regulacji prawnych
W_11	Potrafi wymienić i scharakteryzować wyzwania, zagrożenia i innowacje w obszarze cyberbezpieczeństwa. Zna pojęcie prac badawczo-rozwojowych i jest świadomy ich istotności w branży cyberbezpieczeństwa
UMIEJĘTNOŚCI	
W zakresie umiejętności absolwent potrafi:	
U_01	Potrafi opracować i wdrożyć rozwiązania podnoszące bezpieczeństwo wybranego systemu operacyjnego wraz z aplikacjami, które umożliwiają utworzenie bezpiecznego środowiska pracy
U_02	Stosuje w stopniu podstawowym działania prewencyjne i defensywne w aspekcie bezpieczeństwa systemów cybernetycznych
U_03	Potrafi zaplanować i przeprowadzić testy penetracyjne systemu cyberfizycznego oraz sporządzić dokumentację i raport podatności na atak dla testowanego systemu cyberfizycznego
U_04	Zna techniki Białego Wywiadu (OSINT) i potrafi je wykorzystać do gromadzenia informacji w kontekście testów bezpieczeństwa
U_05	Potrafi dobrać i zastosować skuteczne metody przeciwdziałania atakom skierowanym na infrastrukturę, systemy teleinformatyczne oraz cyberfizyczne
U_06	Potrafi dokonać analizy oraz wyciągnąć wnioski z logów systemowych lub pochodzących z zewnętrznego oprogramowania
U_07	Potrafi stosować procesy informatyki śledczej w celu zabezpieczania i wyodrębniania danych post mortem oraz LIVE, inicjując odpowiednie środki ochronne
U_08	Potrafi zaprojektować i wdrożyć bezpieczny system teleinformatyczny
U_09	Potrafi zdefiniować wymagania i wskaźniki oraz zaplanować i wdrożyć rekrutację specjalistów w zakresie cyberbezpieczeństwa. Potrafi skutecznie zorganizować i zarządzać zespołami projektowymi z wykorzystaniem obecnych na rynku metodyk
U_10	Potrafi wyznaczać cele i układać strategie zapewnienia i utrzymania cyberbezpieczeństwa w jednostce organizacyjnej

KOMPETENCJE W zakresie kompetencji społecznych absolwent jest gotów do:	
K_01	Rozumie problemy i zagrożenia związane z cyberbezpieczeństwem w kontekście technologicznym, prawnym i społecznym
K_02	Rozumie znaczenie socjotechniki w aspekcie wykorzystywania jej przez cyberprzestępców
K_03	Jest świadomy stosowania wymagań prawnych związanych z przetwarzaniem danych osobowych w kontekście implementowanych rozwiązań technologicznych i postaw etycznych w zakresie wyzwań w cyberbezpieczeństwie
K_04	Rozumie wyzwania związane z przetwarzaniem danych osobowych jak i zagrożenia wynikające z braku ochrony prywatności

3. Opis programu studiów

3.1 *Liczba semestrów i liczba punktów ECTS konieczna dla uzyskania kwalifikacji podyplomowych*

Studia trwają dwa semestry. Liczba punktów ECTS wymagana do uzyskania kwalifikacji podyplomowych wynosi 30.

3.2 *Moduły kształcenia - zajęcia lub grupy zajęć - wraz z przypisaniem do każdego modułu zakładanych efektów kształcenia oraz liczby punktów ECTS*

NAZWA PRZEDMIOTU	ECTS	Zakładane efekty uczenia się
Kryptograficzna ochrona danych	2	W_01, W_02, K_01
Podstawy prawne cyberbezpieczeństwa	2	W_03, W_04, K_01
Bezpieczeństwo w systemach teleinformatycznych I	3	W_05, W_06, U_01, U_02, K_02
Atakowanie i ochrona systemów cyberfizycznych I	3	W_02, W_06, U_03, U_04, K_02
Zarządzanie operacjami bezpieczeństwa	2	W_02, W_04, W_07, W_08
Zarządzanie ryzykiem	2	W_06, W_08, W_09,
Bezpieczeństwo w systemach teleinformatycznych II	3	W_02, W_05, U_05, U_06
Atakowanie i ochrona systemów cyberfizycznych II	3	W_04, W_06, U_05, U_07
Architektura systemów cyberbezpiecznych	3	W_02, U_08
Ochrona danych osobowych i informacji niejawnych	2	W_10, K_03, K_04
Zarządzanie zespołem i strategiami cyberbezpieczeństwa	3	U_09, U_10,
Innowacje i wyzwania w cyberbezpieczeństwie	2	W_11, K_01

NAZWA PRZEDMIOTU	ECTS	Zakładane efekty uczenia się
	30	

3.3 Sposoby weryfikacji zakładanych efektów kształcenia osiągniętych przez słuchacza

Metody weryfikacji założonych efektów uczenia się dla studiów podyplomowych określone zostały w sylabusach poszczególnych przedmiotów. Efekty uczenia się w kategorii wiedzy weryfikowane są z wykorzystaniem sprawdzianów. Weryfikacja osiągniętych efektów uczenia się w kategorii umiejętności odbywa się następującymi metodami: bezpośredniej obserwacji uczestnika studiów podyplomowych w czasie wykonywania działań właściwych dla danego zadania oraz projektów. Ocena kompetencji społecznych realizowana będzie za pomocą dyskusji i wypowiedzi pisemnej.

3.4 Plan studiów

NAZWA PRZEDMIOTU	FORMA ZAJĘĆ	LICZBA GODZIN	ECTS	FORMA ZALICZENIA	SEMESTR
Kryptograficzna ochrona danych	WYKŁAD/WARSZTATY	4/8	2	ZO	1
Podstawy prawne cyberbezpieczeństwa	WYKŁAD/WARSZTATY	4/6	2	ZO	1
Bezpieczeństwo w systemach teleinformatycznych I	WYKŁAD/WARSZTATY	7/14	3	ZO	1
Atakowanie i ochrona systemów cyberfizycznych I	WARSZTATY	22	3	ZO	1
Zarządzanie operacjami bezpieczeństwa	WYKŁAD/WARSZTATY	4/6	2	ZO	1
Zarządzanie ryzykiem	WARSZTATY	10	2	ZO	1
Bezpieczeństwo w systemach teleinformatycznych II	WARSZTATY	20	3	ZO	2
Atakowanie i ochrona systemów cyberfizycznych II	WARSZTATY	20	3	ZO	2
Architektura systemów cyberbezpiecznych	WARSZTATY	20	3	ZO	2
Ochrona danych osobowych i informacji niejawnych	WARSZTATY	12	2	ZO	2
Zarządzanie zespołem i strategiami cyberbezpieczeństwa	ĆWICZENIA	20	3	ZO	2
Innowacje i wyzwania w cyberbezpieczeństwie	WYKŁAD	13	2	ZO	2
Razem		190	30		

3.5 Warunki ukończenia studiów podyplomowych

Warunkiem zakończenia studiów podyplomowych jest uzyskanie pozytywnych ocen ze wszystkich przedmiotów realizowanych w planie studiów.

3.6 Wymiar, zasady i formę odbywania praktyk, w przypadku, gdy program kształcenia przewiduje praktyki

Program nie obejmuje realizacji praktyk.

4. Opis warunków prowadzenia i realizacji programu studiów podyplomowych

4.1 Kadra dydaktyczna

Kadrę dydaktyczną stanowią nauczyciele akademicki zatrudnieni w Instytucie Sterowania i Systemów Informatycznych Uniwersytetu Zielonogórskiego dysponujący właściwym doświadczeniem zawodowym w zakresie kształcenia i badań naukowych oraz wysokiej klasy specjaliści z branży IT posiadający wieloletnie doświadczenie w zakresie cyberbezpieczeństwa. Ponadto do kadry dydaktycznej zalicza się specjalistów z zakresu prawa oraz przedstawicieli instytucji i firm, w których wdrożenie wysokiej jakości procedur cyberbezpieczeństwa ma krytyczne znaczenie dla sprawnego funkcjonowania wykorzystywanych w nich systemów i zasobów. W skład zespołu realizującego zajęcia wchodzi osoby, które mają doświadczenie w realizacji prac zespołowych i kształtowaniu umiejętności w zakresie organizacji i pracy zespołu. Jak również nauczyciele akademicki posiadający kompetencje w zakresie budowania infrastruktury sieciowej. Ponadto w skład kadry dydaktycznej wchodzi wysokiej klasy eksperci – reprezentanci firm, które specjalizują się w obszarze budowania bezpieczeństwa cyfrowego.

4.2 Baza dydaktyczna (jeśli jest specyficzna dla studiów podyplomowych)

Zajęcia odbywać się będą w salach Uniwersytetu Zielonogórskiego (Instytut Sterowania i Systemów Informatycznych) wyposażonych w niezbędny do zrealizowania efektów uczenia się sprzęt komputerowy oraz oprogramowanie. Rozwiązania niezbędne do realizacji zajęć i osiągnięcia efektów uczenia się zostaną

r
ó
w
n
i
e
ż

u
d
o
s
t
ę
p
n
i
o
n
e

p