UNIWERSYTET DSW IDEIS
WYDZIAŁ STUDIÓW STOSOWANYCH WE WROCŁAWIU

PROGRAM STUDIÓW
NA KIERUNKU
Zarządzanie cyberbezpieczeństwem
STUDIA DRUGIEGO STOPNIA
PROFIL: PRAKTYCZNY
obowiązujący dla cyklu
rozpoczynającego się w roku akademickim 2026/2027

Spis treści

1. Informacje ogólne

Nazwa kierunku studiów	ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM	
Poziom studiów	studia drugiego stopnia	
Poziom kwalifikacji	7	
Profil studiów	praktyczny	
Forma studiów	Stacjonarne / niestacjonarne	
Kod ISCED	0413	
Liczba semestrów konieczna do ukończenia studiów na ocenianym kierunku na danym poziomie	4	
Liczba punktów ECTS konieczna do ukończenia studiów na ocenianym kierunku na danym poziomie	120	
Łączna liczba godzin zajęć	stacjonarne 1750 godz.	niestacjonarne 1100 godz.
Wymiar praktyk zawodowych	480 godz.	
Język, w którym prowadzone są zajęcia	j. polski	
Tytuł zawodowy uzyskiwany przez absolwenta	Magister	
Uzyskiwane uprawnienia zawodowe	Brak	

2. Zasady rekrutacji i szczegółowy opis wymagań dla kandydatów na studia

Wstęp na studia jest wolny. Warunkiem przyjęcia na studia drugiego stopnia na kierunku „Zarządzanie cyberbezpieczeństwem" jest złożenie kompletu dokumentów rekrutacyjnych, podpisanie umowy o warunkach odpłatności za studia oraz uiszczenie opłaty wpisowej. Kandydat, który złożył komplet wymaganych dokumentów, otrzymuje decyzję o przyjęciu na studia.

Podstawą przyjęcia na studia drugiego stopnia jest dyplom ukończenia studiów pierwszego lub drugiego stopnia albo jednolitych studiów magisterskich. O przyjęcie mogą ubiegać się w szczególności absolwenci kierunków z obszaru nauk o zarządzaniu i jakości oraz nauk o bezpieczeństwie, a także absolwenci innych kierunków biznesowych i technicznych, których dotychczasowe wykształcenie umożliwia uzupełnienie brakujących efektów uczenia się w toku studiów.

- Absolwenci innych kierunków studiów z pierwszego lub drugiego stopnia ubiegający się o studia drugiego stopnia na kierunku zarządzanie cyberbezpieczeństwem są zobligowani do realizacji dodatkowych przedmiotów umożliwiających osiągnięcie zakładanych efektów uczenia się: Podstawy zarządzania i ładu korporacyjnego -16h; Wprowadzenie do bezpieczeństwa informacji i regulacji w cyberbezpieczeństwie -16h.
- Zasady rekrutacji na kierunek „Zarządzanie cyberbezpieczeństwem" są zgodne z ogólnymi zasadami obowiązującymi na pozostałych kierunkach studiów drugiego stopnia prowadzonych na Uniwersytecie Dolnośląskim DSW i zostały określone w Uchwale Senatu. Konstrukcja programów umożliwia płynne

przejście z licencjatu (profil operacyjny) na magisterium (profil strategiczno-przywódczy), przy jednoczesnym otwarciu na absolwentów innych kierunków.

Dodatkowo Uczelnia stworzyła preferencyjne warunki rekrutacji dla finalistów i laureatów olimpiad wskazanych w warunkach rekrutacji.

Opłaty związane z postępowaniem rekrutacyjnym są określone uchwałą Senatu. Decyzje o przyjęciu na studia wydaje Rektor Uczelni poprzez wpis na listę studentów.

3. Przyporządkowanie programu studiów dla kierunku do dyscyplin oraz procentowy udział liczby punktów ECTS każdej z tych dyscyplin w liczbie punktów ECTS koniecznej do ukończenia studiów na ocenianym kierunku na danym poziomie, ze wskazaniem dyscypliny wiodącej.

Nazwa dyscypliny wiodącej, do której został przyporządkowany kierunek:

Nazwa dyscypliny wiodącej	**Punkty ECTS**	
	liczba	**%**
Nauki o zarządzaniu i jakości	72	60%

Nazwy pozostałych dyscyplin wraz z określeniem procentowego udziału liczby punktów ECTS dla pozostałych dyscyplin w ogólnej liczbie punktów ECTS wymaganej do ukończenia studiów na kierunku:

Nazwa dyscypliny	**Punkty ECTS**	
	liczba	**%**
Nauki o bezpieczeństwie	48	40%

4. Podstawowe wskaźniki ECTS określone dla programu studiów

Nazwa wskaźnika	**Liczba punktów ECTS/Liczba godzin**	
	stacjonarne	niestacjonarne
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	39,6 (33%)	39,6 (33%)
Łączna liczba punktów ECTS przyporządkowana zajęciom kształtującym umiejętności praktyczne	88,3 (74%)	88,3 (74%)
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne	6	6
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk społecznych – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki społeczne	n/a	n/a
Łączna liczba punktów ECTS przyporządkowana zajęciom do wyboru	41 (34%)	41 (34%)
Łączna liczba punktów ECTS przyporządkowana praktykom zawodowym	19	19
W przypadku stacjonarnych studiów drugiego stopnia i jednolitych studiów magisterskich liczba godzin zajęć z wychowania fizycznego	n/a	n/a
W przypadku prowadzenia zajęć z wykorzystaniem metod i technik kształcenia na odległość:		

Łączna liczba godzin zajęć określona w programie studiów na studiach stacjonarnych / Łączna liczba godzin zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	1. 1750/94	2. 1100/94

5. Sylwetka absolwenta

Absolwent kierunku Zarządzanie cyberbezpieczeństwem posiada pogłębioną wiedzę z zakresu zarządzania bezpieczeństwem informacji, przywództwa cyfrowego oraz integracji systemów zgodności i ryzyka w realiach regulacyjnych Unii Europejskiej (m.in. NIS2, GDPR/RODO, DORA, AI Act). Dysponuje umiejętnością samodzielnego planowania, wdrażania i doskonalenia rozwiązań w obszarze bezpieczeństwa cyfrowego, łącząc perspektywę prawną, organizacyjną, technologiczną i ludzką. Pełni rolę łącznika pomiędzy zarządem, działami IT, jednostkami biznesowymi oraz interesariuszami zewnętrznymi, wspierając podejmowanie decyzji strategicznych w obszarze bezpieczeństwa i zgodności.

- Potrafi projektować i wdrażać strategie bezpieczeństwa informacji, kierować interdyscyplinarnymi zespołami, nadzorować procesy audytowe oraz budować odporność cyfrową (resilience) organizacji. Wykazuje rozwinięte kompetencje analityczne w zakresie oceny ryzyka, zarządzania incydentami i projektowania systemów monitorowania oraz wskaźników efektywności (KPI/KRI) w obszarze bezpieczeństwa. Jest przygotowany do kształtowania kultury bezpieczeństwa, rozwijania kompetencji pracowników oraz komunikowania ryzyka i rekomendacji na poziomie zarządczym.
- Absolwent jest przygotowany do samodzielnego pełnienia funkcji kierowniczych, doradczych i eksperckich w jednostkach sektora publicznego, finansowego, technologicznego, produkcyjnego oraz w organizacjach międzynarodowych -wszędzie tam, gdzie bezpieczeństwo informacji, systemów cyfrowych i zgodność regulacyjna stanowią strategiczne obszary działalności. Potrafi skutecznie działać w środowisku międzynarodowym, posługując się językiem obcym na poziomie co najmniej B2 według Europejskiego Systemu Opisu Kształcenia Językowego (ESOKJ).

Specjalność: Zarządzanie Bezpieczeństwem Sztucznej Inteligencji (AI Security Governance and Management)

- Specjalność koncentruje się na zarządzaniu ryzykiem, zgodnością prawną i etyką w kontekście projektowania, trenowania, wdrażania i nadzoru systemów sztucznej inteligencji. Program kształtuje kompetencje w zakresie wdrażania norm i standardów międzynarodowych, takich jak ISO/IEC 27001, ISO/IEC 42001 oraz ISO 31000. Absolwent rozumie pełny cykl życia systemów AI oraz ich wpływ na bezpieczeństwo danych, procesów organizacyjnych i relacje z interesariuszami.
- Absolwent tej specjalności potrafi m.in. opracowywać i wdrażać polityki bezpieczeństwa AI, analizować ryzyka związane z modelami AI, przeprowadzać audyty zgodności z wymogami unijnymi (AI Act, GDPR, NIS2), tworzyć mechanizmy nadzoru oraz wspierać zarządy w podejmowaniu decyzji dotyczących wdrożeń AI. Potencjalne stanowiska: AI Security Governance Specialist, AI Risk and Compliance Officer, AI Act Compliance Manager, AI Ethics & Risk Consultant, AI Cybersecurity Advisor.

Specjalność: Zarządzanie Audytami i Jakością w Bezpieczeństwie Informacji (Information Security Audits and Quality Management)

- Specjalność rozwija kompetencje menedżerskie i analityczne w zakresie prowadzenia audytów bezpieczeństwa informacji, zarządzania ryzykiem, zgodnością prawną (compliance) oraz jakością procesów w środowisku cyfrowym. Program łączy wiedzę z zakresu systemów zarządzania bezpieczeństwem informacji (ISO/IEC 27001), jakości (ISO 9001), ciągłości działania (ISO 22301) oraz zarządzania ryzykiem (ISO 31000).
- Absolwent tej specjalności potrafi m.in. projektować i wdrażać system ISMS w oparciu o ISO 27001, prowadzić audyty bezpieczeństwa informacji i zgodności organizacyjnej, identyfikować niezgodności i opracowywać plany działań korygujących, przygotowywać raporty z audytów dla kierownictwa oraz

przygotowywać organizacje do certyfikacji ISO 27001, ISO 9001 i audytów DORA/NIS2. Potencjalne stanowiska: Information Security Auditor, Quality & Compliance Manager, IT/IS Audit Team Lead, DPO -Data Protection Officer, Compliance Specialist, Digital Internal Auditor.

I. Koncepcja kształcenia

1. Wskazanie związku kierunku studiów z misją i strategią rozwoju Uczelni

Przy formułowaniu koncepcji kształcenia na kierunku zarządzanie cyberbezpieczeństwem studia drugiego stopnia o profilu praktycznym uwzględniono:

- misję i strategię Uczelni,
- doświadczenie Uczelni, jej zasoby i możliwość realizacji opracowanej koncepcji kształcenia,
- potrzeby rynku pracy oraz otoczenia społeczno-gospodarczego,
- obowiązujące regulacje prawne i wzorce międzynarodowe,
- opinie interesariuszy zewnętrznych oraz wewnętrznych.

Koncepcja kształcenia na wnioskowanym kierunku jest spójna z misją i strategią Uczelni określoną w „Strategii Uniwersytetu Dolnośląskiego DSW na lata 2022-2025 z perspektywą do 2030 roku" oraz założeniami do strategii Uniwersytetu DSW Ideis na lata 2026 – 2030 z perspektywą do 2035 roku. 1.04.2026 Uniwersytet Dolnośląski DSW zmienił nazwę na Uniwersytet DSW Ideis, a wraz z tą zmianą, uległa modyfikacji strategia długoterminowa, choć atrybuty marki pozostały niezmienne. Uniwersytet DSW dąży do tego, aby być Uczelnią, która jest *miejscem dla Ciebie*, gdzie zgodnie z przyjętą misją łączy się ludzi, kształci praktycznie i realizuje pasje. DSW jest przestrzenią kształtowaną z myślą o studentach jako kluczowej grupie społeczności akademickiej. Uczelnia tworzy przestrzeń do praktycznej nauki, pracy, współdziałania, rozwoju wspólnie we współpracy z kolegami i koleżankami, jak również z wykładowcami, którzy wspierają studentów na każdym etapie edukacji. Jest to też miejsce zapewniające warunki do samorozwoju, realizacji zainteresowań, poznawania ciekawych ludzi, budowania i pielęgnowania relacji oraz kreowania i współtworzenia. Uniwersytet to miejsce, w którym doświadcza się inspiracji, wzajemnego uczenia się, uczenia innych i wymiany praktycznych doświadczeń. Wizja Uczelni brzmi: „w przyjaznej przestrzeni wspólnie rozwijamy usługę edukacyjną opartą na wiedzy, najlepszej praktyce i nowoczesnej technologii".

Społeczność akademicką tworzą wykładowcy otwarci, zaangażowani, pełni wiedzy i doświadczeń, którą chcą się dzielić oraz inspirować studentów i współpracowników do poznawania i odkrywania otaczającego nas świata. Uniwersytet DSW Ideis jest uczelnią akademicką, która aktywnie współtworzy Federację Naukową WSB-DSW Merito i wspiera rozwój naukowy w wybranych dyscyplinach. We właśnie zakończonej ewaluacji jakości działalności naukowej uczelni, której zostały poddane dyscypliny rozwijane przez uczelnie należące do Federacji Naukowej, kluczowe dla wnioskowanego kierunku dyscypliny: ekonomia i finanse oraz nauki o zarządzaniu i jakości uzyskały najwyższe oceny „A". DSW świadomie kształtuje swoją tożsamość, łącząc doświadczenia w zakresie kształcenia i prowadzenia nauki, wartości (takie jak współpraca, zaangażowanie, wiarygodność, kreatywność, innowacyjność, elastyczność, otwartość) oraz podstawy modelu biznesowego członka Grupy TEB Akademia i Federacji Naukowej WSB-DSW Merito z wizją dynamicznego rozwoju uczelni w modelu PUMA (Praktyczność Uniwersalność Masowość Akademickość).

Zarówno misja, jak i wizja wytyczają strategiczne kierunki działań w rozwoju Uczelni, który został ukierunkowany m.in. na poszerzenie działań edukacyjnych o obszar zarządzania cyberbezpieczeństwem. W ramach realizacji tego założenia, w oparciu o szczegółowe analizy rynku, Uniwersytet DSW Ideis wprowadziła do oferty edukacyjnej kierunek studiów zarządzanie cyberbezpieczeństwem, którego koncepcja kształcenia spełnia zarówno oczekiwania rynku, jak i samych studentów, odpowiadając na ich potrzeby oraz pasje.

Aktywna praca Biura Karier, kojarzącego studentów i absolwentów z rynkiem i pracodawcami, to kolejny element strategicznych działań Uniwersytetu, który będzie koncentrował się na nowych miejscach pracy dla absolwentów, w których możliwe jest wykorzystanie wiedzy z zakresu zarządzania cyberbezpieczeństwem, compliance, audytu IT i bezpieczeństwa informacji, m.in. w takich miejscach jak: działy bezpieczeństwa informacji w przedsiębiorstwach, instytucje regulacyjne i nadzorcze, firmy konsultingowe ds. cyberbezpieczeństwa,

instytucje finansowe z wyodrębnionymi działami bezpieczeństwa cyfrowego, przedsiębiorstwa technologiczne, administracja publiczna oraz instytucje doradcze i think-tanki zajmujące się strategicznym bezpieczeństwem.

2. Wskazanie potrzeb społeczno-gospodarczych utworzenia studiów oraz zgodności efektów uczenia się z tymi potrzebami

Zarządzanie cyberbezpieczeństwem na poziomie magisterskim to odpowiedź na rosnące zapotrzebowanie rynku pracy na liderów i ekspertów strategicznych -osoby, które nie tylko znają narzędzia obrony cyfrowej, lecz potrafią zarządzać ryzykiem, projektować polityki bezpieczeństwa i odpowiadać na wymogi regulacyjne na poziomie całej organizacji. Profil absolwenta II stopnia wychodzi naprzeciw potrzebom zarządów i rad nadzorczych, które coraz częściej odpowiadają prawnie za stan cyberbezpieczeństwa swoich instytucji.

Zapotrzebowanie na ekspertów szczebla strategicznego w dziedzinie cyberbezpieczeństwa jest pochodną kilku równoległych trendów. Globalny rynek cyberbezpieczeństwa rośnie w tempie 13,8% rocznie i ma osiągnąć wartość 699 mld USD do 2034 roku. Jednocześnie badanie ISC2 z 2025 roku ujawniło, że kluczowym problemem organizacji nie jest już tylko brak ludzi, ale brak umiejętności: 59% organizacji zgłasza krytyczne lub znaczące luki kompetencyjne (wzrost o 15 punktów procentowych rok do roku), a AI, cloud security, zarządzanie ryzykiem (GRC) i inżynieria bezpieczeństwa figurują jako cztery najczęściej wskazywane obszary niedoborów. Wszystkie te obszary należą do programowego rdzenia studiów II stopnia na kierunku Zarządzanie cyberbezpieczeństwem.

Na poziomie europejskim ENISA potwierdziła w raporcie NIS Investments 2025, że deficyt specjalistów w UE sięgnął 299 000 w 2024 roku (wzrost o 9% r/r), a 76% organizacji ma trudności z pozyskaniem kadry i 71% z jej utrzymaniem -przy jednoczesnym wzroście wskaźników wypalenia zawodowego (burnout nawet u 68% profesjonalistów cyberbezpieczeństwa). World Economic Forum w Global Cybersecurity Outlook 2026 podkreśla, że „sieci i cyberbezpieczeństwo" zajmują miejsce wśród trzech najszybciej rosnących kategorii umiejętności do 2030 roku, zaraz po AI i big data (WEF Global Cybersecurity Outlook 2026). Zapotrzebowanie na role strategiczne -CISO, Lead Auditor, Head of Information Security, DPO -wzrasta przy tym szybciej niż na stanowiska operacyjne, co bezpośrednio uzasadnia kształcenie na poziomie magisterskim.

Decydującym czynnikiem kształtującym popyt na specjalistów II stopnia jest nowa architektura regulacyjna Unii Europejskiej. Rozporządzenie DORA (Digital Operational Resilience Act), obowiązujące od stycznia 2025 roku, nakłada na sektor finansowy konkretne obowiązki w zakresie odporności operacyjnej, testowania TLPT i zarządzania ryzykiem stron trzecich, a za naruszenia grożą kary do 1% dziennego obrotu. Dyrektywa NIS2 w ramach nowelizacji UKSC obejmie w Polsce kilka tysięcy nowych podmiotów -z wymogiem posiadania wyznaczonego, kompetentnego kierownika ds. cyberbezpieczeństwa odpowiedzialnego przed zarządem. Do tego dochodzi rozporządzenie AI Act, które tworzy nową warstwę wymogów w zakresie zarządzania ryzykiem systemów AI, wchodząc w życie etapowo do 2027 roku. Szacuje się, że w Europie regulacje te przekładają się na wzrost popytu na specjalistów compliance i GRC: blisko 50% europejskich organizacji przyznaje, że regulacje compliance bezpośrednio kształtują ich bieżące decyzje kadrowe. W Polsce wdrożenie NIS2 i DORA wymusi zatrudnienie tysięcy dodatkowych ekspertów ds. bezpieczeństwa informacji i audytu w sektorze finansowym, energetycznym, administracji publicznej i infrastrukturze krytycznej.

W Polsce rynek cyberbezpieczeństwa wyceniano na 1,52 mld USD pod koniec 2024 roku, z prognozowanym wzrostem 5,85% rocznie do 2029 roku. Dolny Śląsk, z Wrocławiem jako trzecim co do wielkości centrum nowoczesnych usług biznesowych w Polsce (70 300 pracowników w sektorze BSS w I kw. 2025 r., ABSL 2025), jest naturalnym miejscem kształcenia kadr dla tej branży. Blisko połowa polskich centrów usług biznesowych świadczy usługi cyberbezpieczeństwa, a instytucje takie jak EY GDS Poland, Accenture, Fidelity, Smith & Nephew, ArcelorMittal czy Ernst & Young aktywnie rekrutują we Wrocławiu na stanowiska Senior Security Consultant, IT

Audit Manager i GRC Specialist. Raport płacowy Devire wskazuje, że specjaliści ds. cyberbezpieczeństwa należą we Wrocławiu do grupy najlepiej wynagradzanych w całym sektorze IT, a Senior Security Engineer może zarabiać 25–30 tys. PLN miesięcznie (B2B). Raporty rekrutacyjne Devire za 2025 rok potwierdzają, że specjaliści z kompetencjami AI security, GRC i cloud security należą do najtrudniejszych do pozyskania na rynku dolnośląskim.

Sztuczna inteligencja staje się osobnym wektorem ryzyka i jednocześnie kompetencyjnym priorytetem. W badaniu ISC2 z 2025 roku AI wskazano jako największą lukę umiejętności (41% respondentów), a 73% specjalistów uważa, że AI będzie wymagała bardziej wyspecjalizowanych kompetencji w zakresie cyberbezpieczeństwa. Specjalność „Zarządzanie Bezpieczeństwem Sztucznej Inteligencji" realizowana w ramach programu studiów II stopnia bezpośrednio odpowiada na ten niedobór, przygotowując absolwentów do wdrażania AI Act, oceny ryzyka modeli AI oraz audytu systemów opartych na uczeniu maszynowym.

Uniwersytet DSW Ideis, wychodzi naprzeciw tym potrzebom, opracowując program studiów II stopnia na kierunku „Zarządzanie cyberbezpieczeństwem" jako kształcenie kadr liderskich. Podział dyscyplinowy 60% (nauki o zarządzaniu i jakości) / 40% (nauki o bezpieczeństwie) oraz dwie specjalności -Zarządzanie Bezpieczeństwem Sztucznej Inteligencji i Zarządzanie Audytami i Jakością w Bezpieczeństwie Informacji -zostały zaprojektowane tak, by wypełniać konkretną lukę rynkową: brak specjalistów zdolnych zarówno do strategicznego zarządzania bezpieczeństwem, jak i do technicznej oceny zgodności z NIS2, DORA i AI Act. Partnerstwo z Defence Institute - instytucją doradczą w obszarze bezpieczeństwa narodowego i cyberprzestrzeni, współtworzoną przez doświadczonych ekspertów wojskowych i akademickich -zapewnia studentom dostęp do unikalnej perspektywy strategicznej i kontaktów w środowisku instytucji bezpieczeństwa państwa.

Kierunek łączy dwa obszary dyscyplinarne: nauki o zarządzaniu i jakości (60% ECTS) oraz nauki o bezpieczeństwie (40% ECTS), tworząc unikalny profil kształcenia ukierunkowany na zarządzanie strategiczne i przywództwo w bezpieczeństwie cyfrowym. Absolwenci są przygotowani do pełnienia ról eksperckich takich jak CISO (Chief Information Security Officer), Lead Auditor, AI Risk Officer czy Compliance Manager.

Koncepcja studiów II stopnia uwzględnia dwie główne grupy odbiorców: absolwentów studiów I stopnia „Zarządzanie cyberbezpieczeństwem" kontynuujących kształcenie na poziomie strategiczno-przywódczym, oraz absolwentów innych kierunków biznesowych i technicznych. Konstrukcja programu umożliwia zarówno pogłębianie kompetencji absolwentów kierunków pokrewnych, jak i bezpieczne wejście i rozwój w obszarze zarządzania cyberbezpieczeństwem dla osób spoza tego obszaru, zgodnie z priorytetami UE w zakresie wzmacniania kompetencji cyfrowych.

Studia II stopnia na kierunku zarządzanie cyberbezpieczeństwem pozwolą studentom:

- poznać i zrozumieć mechanizmy strategicznego zarządzania bezpieczeństwem informacji w organizacjach o różnym profilu działalności;
- samodzielnie projektować, wdrażać i oceniać strategie bezpieczeństwa informacji oraz systemy zarządzania ciągłością działania;
- zdobyć zaawansowane umiejętności nadzorowania auditów i procesów zapewniania zgodności (compliance);
- stosować europejskie regulacje cyberbezpieczeństwa (NIS2, DORA, AI Act, RODO) w praktyce organizacyjnej;
- kierować interdyscyplinarnymi zespołami ds. bezpieczeństwa oraz skutecznie komunikować się z organami regulacyjnymi;
- krytycznie oceniać istniejące i proponować nowe rozwiązania zarządcze i techniczne w obszarze cyberbezpieczeństwa;
- etycznie i odpowiedzialnie zarządzać technologiami cyfrowymi, w tym sztuczną inteligencją, z uwzględnieniem złożonych uwarunkowań prawnych i społecznych.

Efekty uczenia się opracowane dla kierunku wpisują się w dziedzinę nauk społecznych i nauk o bezpieczeństwie. Mają charakter praktyczny (profil praktyczny) i odpowiadają wymaganiom poziomu 7 Polskiej Ramy Kwalifikacji (PRK). Dzięki zastosowaniu różnorodnych form kształcenia -konwersatoriów, seminariów, warsztatów, projektów, studiów przypadków oraz symulacji -studenci rozwijają zaawansowane umiejętności praktyczne niezbędne w środowiskach zarządzania bezpieczeństwem.

Należy wskazać, że tak opracowana koncepcja kształcenia wpisuje się w jeden z celów strategicznych Strategii Rozwoju Województwa Dolnośląskiego 2030: Wzmocnienie regionalnego kapitału ludzkiego i społecznego i wskazane w nim do realizacji zadania, m.in.: kształtowanie i rozwój usług edukacyjnych i społecznych ukierunkowanych na rozwój rynków pracy; wsparcie innowacyjnych metod kształcenia; wspieranie działań na rzecz rozwoju umiejętności i postaw kreatywnych i przedsiębiorczych (https://umwd.dolnyslask.pl/fileadmin/user_upload/Organizacje_pozarzadowe/SRWD_2030_calosc_druk.pdf [2026-04-03]).

Na podkreślenie zasługuje fakt, że w trakcie pracy nad koncepcją kierunku i modułami przedmiotów wybieralnych, prowadzone były konsultacje z przedstawicielami otoczenia społeczno-ekonomicznego. Koncepcja programu studiów była współtworzona i konsultowana z instytucjami działającymi w obszarze zarządzania cyberbezpieczeństwem.

Swoistą egzemplifikacją związku Uczelni z otoczeniem społeczno-gospodarczym są realizowane projekty badawczo-rozwojowe.

Wysokie kompetencje dydaktyczne nauczycieli akademickich prowadzących zajęcia na kierunku, poparte osiągnięciami w pracy naukowej oraz doświadczeniem praktycznym, zapewniają wysoką jakość kształcenia. Kadra wykładowców to głównie doświadczeni praktycy -specjaliści z zakresu zarządzania cyberbezpieczeństwem, ochrony danych, audytu bezpieczeństwa informacji, zgodności (compliance) i prawa cyfrowego -oraz dydaktycy o znaczącym dorobku naukowym posiadający również doświadczenie w praktyce.

Doświadczenie zdobyte poza uczelnią wykorzystują w pracy dydaktycznej, wskazując studentom konkretne przykłady zastosowania wiedzy teoretycznej w praktyce. Umowy z partnerami zewnętrznymi dotyczące organizacji praktyk studenckich oraz prowadzenia zajęć przez osoby posiadające znaczące pozaakademickie doświadczenie zawodowe, zapewniają studentom bezpośredni kontakt z praktykami i umożliwiają poznanie różnych profesji, w których umiejętności zdobywane podczas studiów znajdują zastosowanie.

Absolwent kierunku zarządzanie cyberbezpieczeństwem jest otwarty na zmiany, wyposażony w umiejętności dostosowywania się do zmieniającego się otoczenia cyfrowego i regulacyjnego, w tym rynku pracy. Cechuje się etyczną i społeczną odpowiedzialnością zawodową. Docenia znaczenie całożyciowego uczenia się i jest przygotowany do kontynuowania edukacji na studiach podyplomowych i MBA.

3. Ogólne cele uczenia się

Studia II stopnia na kierunku „Zarządzanie cyberbezpieczeństwem" realizowane są w profilu praktycznym i kształcą liderów oraz ekspertów zdolnych do strategicznego zarządzania bezpieczeństwem informacji w złożonych, dynamicznych warunkach organizacyjnych i regulacyjnych. Program pogłębia kompetencje zarządcze i analityczne, integrując zaawansowaną wiedzę z zakresu ładu korporacyjnego w obszarze bezpieczeństwa (governance), zarządzania ryzykiem, audytu, ciągłości działania, zapewnienia zgodności (compliance) oraz bezpiecznego wykorzystania technologii sztucznej inteligencji. Jest skierowany zarówno do absolwentów I stopnia kierunku „Zarządzanie cyberbezpieczeństwem", jak i do absolwentów pokrewnych kierunków biznesowych i technicznych. Ogólne cele uczenia się na tym kierunku obejmują:

- Ukształtowanie pogłębionej, systemowej wiedzy o strategicznym zarządzaniu cyberbezpieczeństwem i jego otoczeniu regulacyjnym. Absolwent powinien posiadać zaawansowaną, usystematyzowaną wiedzę z zakresu ładu korporacyjnego w obszarze bezpieczeństwa, zarządzania ryzykiem cyfrowym, europejskich i krajowych regulacji (NIS2, DORA, AI Act, RODO/GDPR) oraz odpowiedzialności organów zarządczych za stan bezpieczeństwa organizacji. Wiedza ta wykracza poza poziom operacyjny i obejmuje rozumienie mechanizmów systemowych, strategicznych zależności między decyzjami zarządczymi a odpornością cyfrową organizacji oraz zdolność do interpretowania i stosowania norm i standardów międzynarodowych (m.in. ISO/IEC 27001, ISO 31000, ISO/IEC 42001).

- Przygotowanie do samodzielnego projektowania, wdrażania i oceny strategii bezpieczeństwa informacji oraz systemów zarządzania odpornością cyfrową. Absolwent powinien potrafić samodzielnie zaprojektować, wdrożyć i doskonalić strategię bezpieczeństwa informacji dostosowaną do specyfiki organizacji, jej profilu ryzyka i otoczenia regulacyjnego. Cel ten obejmuje zdolność do budowania systemów zarządzania ciągłością działania (BCM), projektowania mechanizmów zarządczych, wskaźników efektywności (KPI/KRI) oraz rekomendowania rozwiązań dla kadry zarządzającej — z uwzględnieniem zarówno perspektywy prawnej i organizacyjnej, jak i technologicznej.

- Wyposażenie w zaawansowane umiejętności kierowania zespołami, nadzorowania audytów i zarządzania zgodnością (compliance) w zmiennym otoczeniu regulacyjnym. Absolwent powinien być przygotowany do kierowania interdyscyplinarnymi zespołami ds. bezpieczeństwa, planowania i koordynowania złożonych reakcji na incydenty, nadzorowania procesów audytowych oraz zarządzania zgodnością z wymaganiami regulatorów i organów nadzorczych. Szczególny nacisk kładzie się na umiejętność prowadzenia współpracy z interesariuszami wewnętrznymi (zarząd, dział prawny, IT, HR) i zewnętrznymi (CSIRT, organy regulacyjne, audytorzy zewnętrzni) — co bezpośrednio odpowiada na profile stanowisk CISO, Lead Auditor, DPO oraz Compliance Manager poszukiwanych przez pracodawców na rynku.

- Kształtowanie zdolności do etycznego, krytycznego i odpowiedzialnego zarządzania technologiami cyfrowymi, w tym sztuczną inteligencją. Absolwent powinien być zdolny do oceny ryzyk technologicznych, prawnych i etycznych związanych z wdrożeniem systemów AI, projektowania polityk bezpieczeństwa AI oraz wdrażania wymagań unijnego rozporządzenia AI Act. Cel ten obejmuje rozumienie pełnego cyklu życia systemu AI, jego wpływu na bezpieczeństwo danych i procesów organizacyjnych, a także umiejętność budowania mechanizmów nadzoru, dokumentacji i raportowania zgodności — z poszanowaniem praw człowieka, zasad zrównoważonego rozwoju i długofalowej odpowiedzialności za podejmowane decyzje.

- Przygotowanie do samodzielnego pełnienia zaawansowanych ról eksperckich i przywódczych w obszarze zarządzania bezpieczeństwem informacji. Absolwent powinien być gotowy do objęcia stanowisk kierowniczych, doradczych i eksperckich w organizacjach sektora publicznego, finansowego, technologicznego i produkcyjnego — zarówno w Polsce, jak i w środowisku międzynarodowym (poziom językowy co najmniej B2 ESOKJ). Studia przygotowują do pełnienia ról CISO, Head of Information Security, AI Security Officer, Lead Auditor czy Security Governance Specialist, kształtując jednocześnie gotowość do ciągłego doskonalenia kompetencji w obszarze dynamicznie zmieniającego się krajobrazu zagrożeń, regulacji i technologii.

4. Tabela odniesień efektów kierunkowych uczenia się do charakterystyk kompetencji uniwersalnych Zintegrowanego Systemu Kwalifikacji oraz charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 Polskiej Ramy Kwalifikacji

Objaśnienie oznaczeń w symbolach efektów kierunkowych:	
ZCYB	kierunek zarządzanie cyberbezpieczeństwem
II	studia drugiego stopnia
P	profil praktyczny
W	kategoria wiedzy
U	kategoria umiejętności

K	kategoria kompetencji społecznych
01, 02, 03 i kolejne	numer efektu uczenia się
Objaśnienie oznaczeń charakterystyki poziomów PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego:	
7	poziom 7 Polskiej Ramy Kwalifikacji
S	charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego
W	wiedza
G	głębia i zakres
K	kontekst
U	umiejętności
W	wykorzystanie wiedzy
K	komunikowanie się
O	organizacja pracy
U	uczenie się
K	kompetencje społeczne
K	krytyczna ocena
O	odpowiedzialność
R	rola zawodowa

Objaśnienie oznaczeń:

ZCYB_II_	kierunkowe efekty uczenia się dla studiów drugiego stopnia kierunku ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM (mgr)
W	kategoria wiedzy
U	kategoria umiejętności
K	kategoria kompetencji społecznych
P7S_WG	poziom 7 Polskiej Ramy Kwalifikacji kategoria wiedza: zna i rozumie/zakres i głębia
P7S_WK	poziom 7 Polskiej Ramy Kwalifikacji kategoria wiedza: zna i rozumie/kontekst
P7S_UW	poziom 7 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/wykorzystanie wiedzy
P7S_UK	poziom 7 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/komunikowanie się
P7S_UO	poziom 7 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/organizacja pracy
P7S_UU	poziom 7 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/uczenie się
P7S_KK	poziom 7 Polskiej Ramy Kwalifikacji kategoria kompetencje społeczne: jest gotów do/oceny
P7S_KO	poziom 7 Polskiej Ramy Kwalifikacji kategoria kompetencje społeczne: jest gotów do/odpowiedzialność
P7S_KR	poziom 7 Polskiej Ramy Kwalifikacji kategoria kompetencje społeczne: jest gotów do/rola zawodowa
01, 02, 03 i kolejne	numer efektu uczenia się

Symbol efektu uczenia się dla kierunku	**OPIS KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ Po zakończeniu studiów drugiego stopnia na kierunku zarządzanie cyberbezpieczeństwem, profil praktyczny, absolwent osiąga następujące efekty uczenia się:**	**Symbol charakterystyk**
	WIEDZA -absolwent:	
ZCYB_II_W01	Zna i rozumie w pogłębionym stopniu złożone koncepcje zarządzania organizacją i cyberbezpieczeństwem, uwzględniając ich współczesne ujęcia teoretyczne i praktyczne	P7U_W P7S_WG
ZCYB_II_W02	Zna i rozumie w pogłębionym stopniu modele współpracy interesariuszy oraz polityki bezpieczeństwa w skali międzynarodowej i krajowej	P7U_W P7S_WG

ZCYB_II_W03	Zna i rozumie w pogłębionym stopniu mechanizmy regulacyjne i prawne związane z ochroną danych, cyberbezpieczeństwem i standardami (NIS2, AI Act, DORA, RODO/GDPR)	P7U_W P7S_WG
ZCYB_II_W04	Zna i rozumie w pogłębionym stopniu typologie zagrożeń, ich struktury oraz wpływ na funkcjonowanie organizacji	P7U_W P7S_WG
ZCYB_II_W05	Zna i rozumie w pogłębionym stopniu architekturę systemów zarządzania bezpieczeństwem informacji oraz podstawy technologii kryptograficznych	P7U_W P7S_WG
ZCYB_II_W06	Zna i rozumie w pogłębionym stopniu metodyki zarządzania projektami, zmianą i ryzykiem w środowiskach cyfrowych	P7U_W P7S_WG
ZCYB_II_W07	Zna i rozumie wpływ psychologicznych i społecznych czynników na bezpieczeństwo organizacji i jej pracowników	P7U_W P7S_WK
ZCYB_II_W08	Zna i rozumie znaczenie oraz mechanizmy transformacji cyfrowej i innowacji technologicznych wpływających na bezpieczeństwo organizacji	P7U_W P7S_WK
ZCYB_II_W09	Zna i rozumie w pogłębionym stopniu modele i strategie zarządzania odpornością organizacji na zagrożenia cybernetyczne i kryzysy	P7U_W P7S_WG
ZCYB_II_W10	Zna i rozumie zastosowania sztucznej inteligencji w bezpieczeństwie, jej główne ryzyka oraz normy regulacyjne	P7U_W P7S_WK
ZCYB_II_W11	Zna i rozumie zasady zarządzania zespołami różnorodnymi oraz rozwiązywania konfliktów w kontekście bezpieczeństwa	P7U_W P7S_WK
ZCYB_II_W12	Zna i rozumie w pogłębionym stopniu mechanizmy zapewniania zgodności i audytu bezpieczeństwa zgodne z aktualnymi wymogami prawa i standardami branżowymi	P7U_W P7S_WG
ZCYB_II_W13	Zna i rozumie znaczenie ochrony prywatności oraz zjawiska biasu w systemach sztucznej inteligencji	P7U_W P7S_WK
ZCYB_II_W14	Zna i rozumie w pogłębionym stopniu metody statystyczne i analityczne stosowane w ocenie ryzyka i efektywności strategii bezpieczeństwa	P7U_W P7S_WG
ZCYB_II_W15	Zna i rozumie etyczne i społeczne konsekwencje zarządzania cyberbezpieczeństwem w dobie cyfryzacji i globalizacji	P7U_W P7S_WK
UMIEJĘTNOŚCI -absolwent:		
ZCYB_II_U01	Potrafi samodzielnie tworzyć i wdrażać polityki bezpieczeństwa oraz strategie zarządzania ryzykiem cybernetycznym	P7U_U P7S_UW
ZCYB_II_U02	Potrafi prowadzić złożone analizy strategiczne w organizacjach o różnych profilach działalności	P7U_U P7S_UW
ZCYB_II_U03	Potrafi modelować oraz optymalizować procesy reagowania na incydenty oraz zarządzania ciągłością działania	P7U_U P7S_UW

ZCYB_II_U04	Potrafi realizować i nadzorować audyty bezpieczeństwa informacji zgodne ze standardami i wymaganiami prawnymi	P7U_U P7S_UW
ZCYB_II_U05	Potrafi efektywnie komunikować się oraz współpracować z interesariuszami w środowisku wielosektorowym i międzykulturowym	P7U_U P7S_UK
ZCYB_II_U06	Potrafi wykorzystywać zaawansowane narzędzia IT, w tym rozwiązania oparte na sztucznej inteligencji, do monitoringu, analizy i automatyzacji procesów bezpieczeństwa	P7U_U P7S_UW
ZCYB_II_U07	Potrafi identyfikować luki i zagrożenia w systemach bezpieczeństwa oraz formułować rekomendacje naprawcze	P7U_U P7S_UW
ZCYB_II_U08	Potrafi zarządzać zmianami organizacyjnymi i technologicznymi, minimalizując opór i ryzyko	P7U_U P7S_UO
ZCYB_II_U09	Potrafi prowadzić negocjacje i mediacje w celu utrzymania zgodności i współpracy między zespołami	P7U_U P7S_UK
ZCYB_II_U10	Potrafi przygotowywać raporty strategiczne i analizy dla kierownictwa oraz organów regulacyjnych	P7U_U P7S_UK
ZCYB_II_U11	Potrafi integrować trendy innowacyjne oraz regulacje prawne w procesach podejmowania decyzji zarządczych	P7U_U P7S_UW
ZCYB_II_U12	Potrafi planować i prowadzić działania edukacyjne oraz szkoleniowe w obszarze cyberbezpieczeństwa	P7U_U P7S_UO
ZCYB_II_U13	Potrafi planowo rozwijać własne kompetencje oraz kompetencje zespołu zgodnie z potrzebami rynku i organizacji	P7U_U P7S_UU
ZCYB_II_U14	Potrafi krytycznie oceniać istniejące i proponować nowe rozwiązania zarządcze i techniczne w obszarze cyberbezpieczeństwa	P7U_U P7S_UW
ZCYB_II_U15	Potrafi posługiwać się językiem obcym na poziomie umożliwiającym realizację obowiązków zawodowych w środowisku międzynarodowym, co odpowiada co najmniej poziomowi B2 według Europejskiego Systemu Opisu Kształcenia Językowego	P7U_U P7S_UK
ZCYB_II_U16	Potrafi projektować systemy zarządzania efektywnością i ciągłym doskonaleniem bezpieczeństwa w organizacji	P7U_U P7S_UW
ZCYB_II_U17	Potrafi oceniać efektywność działań organizacji w obszarze ochrony przed zagrożeniami cybernetycznymi	P7U_U P7S_UW
KOMPETENCJE SPOŁECZNE -absolwent:		
ZCYB_II_K01	Jest gotów inicjować, planować i aktywnie realizować działania zespołowe oraz projekty organizacyjne i społeczne z zakresu zarządzania cyberbezpieczeństwem, wspierające rozwój kultury bezpieczeństwa informacji	P7U_K P7S_KO

ZCYB_II_K02	Jest gotów identyfikować potrzeby doskonalenia oraz proponować i wdrażać rozwiązania usprawniające system zarządzania cyberbezpieczeństwem, w tym procedury, procesy i narzędzia, z uwzględnieniem zasad zarządzania jakością	P7U_K P7S_KO
ZCYB_II_K03	Jest gotów brać odpowiedzialność za decyzje podejmowane w złożonych, niejednoznacznych sytuacjach związanych z cyberbezpieczeństwem oraz pełnić rolę lidera zespołu projektowego, operacyjnego lub kryzysowego	P7U_K P7S_KR
ZCYB_II_K04	Jest gotów efektywnie współpracować w zespołach interdyscyplinarnych, uwzględniając różne perspektywy interesariuszy, dbając o poszanowanie różnorodności oraz prowadzenie konstruktywnego dialogu, także w sytuacjach konfliktu lub presji decyzyjnej	P7U_K P7S_KO
ZCYB_II_K05	Jest gotów zapewniać jasną, rzetelną i przejrzystą komunikację w procesach zarządzania cyberbezpieczeństwem, w tym skuteczną koordynację zadań, raportowanie ryzyk i incydentów oraz budowanie zaufania w relacjach wewnętrznych i zewnętrznych	P7U_K P7S_KK

5. Tabela pokrycia charakterystyk kompetencji uniwersalnych Zintegrowanego Systemu Kwalifikacji oraz charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-7 Polskiej Ramy Kwalifikacji przez kierunkowe efekty uczenia się

Symbol charakterystyk	Opis charakterystyk kompetencji uniwersalnych poziomu 6 Zintegrowanego Systemu Kwalifikacji oraz charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji Polskiej Ramy Kwalifikacji	Symbol efektu uczenia się dla kierunku
WIEDZA absolwent zna i rozumie:		
P7U_W	w zaawansowanym stopniu -fakty, teorie, metody oraz złożone zależności między nimi różnorodne, złożone uwarunkowania prowadzonej działalności	ZCYB_II_W01 ZCYB_II_W02 ZCYB_II_W03 ZCYB_II_W04 ZCYB_II_W05
P7S_WG	w zaawansowanym stopniu -wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące podstawową wiedzę ogólną z zakresu dyscyplin naukowych lub artystycznych tworzących podstawy teoretyczne oraz wybrane zagadnienia z zakresu wiedzy szczegółowej -właściwe dla programu studiów, a w przypadku studiów o profilu praktycznym - również zastosowania praktyczne tej wiedzy w działalności zawodowej związanej z ich kierunkiem	ZCYB_II_W01 ZCYB_II_W02 ZCYB_II_W03 ZCYB_II_W04 ZCYB_II_W05
P7S_WK	fundamentalne dylematy współczesnej cywilizacji podstawowe ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej związanej z kierunkiem studiów, w tym podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego podstawowe zasady tworzenia i rozwoju różnych form przedsiębiorczości	ZCYB_II_W07 ZCYB_II_W08 ZCYB_II_W10 ZCYB_II_W11 ZCYB_II_W13
UMIEJĘTNOŚCI absolwent potrafi:		

P7U_U	innowacyjnie wykonywać zadania oraz rozwiązywać złożone i nietypowe problemy w zmiennych i nie w pełni przewidywalnych warunkach samodzielnie planować własne uczenie się przez całe życie komunikować się z otoczeniem, uzasadniać swoje stanowisko	ZCYB_II_U01 ZCYB_II_U02 ZCYB_II_U03 ZCYB_II_U04 ZCYB_II_U05
P7S_UW	wykorzystywać posiadaną wiedzę -formułować i rozwiązywać złożone i nietypowe problemy oraz wykonywać zadania w warunkach nie w pełni przewidywalnych przez: – właściwy dobór źródeł oraz informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy i syntezy tych informacji, – dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych wykorzystywać posiadaną wiedzę -formułować i rozwiązywać problemy oraz wykonywać zadania typowe dla działalności zawodowej związanej z kierunkiem studiów -w przypadku studiów o profilu praktycznym	ZCYB_II_U01 ZCYB_II_U02 ZCYB_II_U03 ZCYB_II_U04 ZCYB_II_U06
P7S_UK	komunikować się z otoczeniem z użyciem specjalistycznej terminologii brać udział w debacie -przedstawiać i oceniać różne opinie i stanowiska oraz dyskutować o nich posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego	ZCYB_II_U05 ZCYB_II_U09 ZCYB_II_U10
P7S_UO	planować i organizować pracę indywidualną oraz w zespole współdziałać z innymi osobami w ramach prac zespołowych (także o charakterze interdyscyplinarnym)	ZCYB_II_U08 ZCYB_II_U12
P7S_UU	samodzielnie planować i realizować własne uczenie się przez całe życie	ZCYB_II_U13
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:		
P7U_K	kultywowania i upowszechniania wzorów właściwego postępowania w środowisku pracy i poza nim samodzielnego podejmowania decyzji, krytycznej oceny działań własnych, działań zespołów, którymi kieruje, i organizacji, w których uczestniczy, przyjmowania odpowiedzialności za skutki tych działań	ZCYB_II_K01 ZCYB_II_K02 ZCYB_II_K03 ZCYB_II_K04 ZCYB_II_K05
P7S_KK	krytycznej oceny posiadanej wiedzy i odbieranych treści uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu	ZCYB_II_K05
P7S_KO	wypełniania zobowiązań społecznych, współorganizowania działalności na rzecz środowiska społecznego inicjowania działania na rzecz interesu publicznego myślenia i działania w sposób przedsiębiorczy	ZCYB_II_K01 ZCYB_II_K02 ZCYB_II_K04
P7S_KR	odpowiedzialnego pełnienia ról zawodowych, w tym: – przestrzegania zasad etyki zawodowej i wymagania tego od innych, – dbałości o dorobek i tradycje zawodu	ZCYB_II_K03

II. Plan studiów

1. Struktura planu studiów

Lp.	Moduły	Liczba godz. studia stacjonarne				Liczba godz. studia niestacjonarne			
		Ogół.	wyk.	ćw.	p/e/ prak.	Ogół.	wyk.	ćw.	p/e/ prak.
1	Moduły kształcenia podstawowego	246	106	126	14	106	28	64	14
2	Moduły kształcenia kierunkowego	550	166	354	30	250	76	144	30
3	Moduły przygotowania pracy dyplomowej	108	0	98	10	62	0	52	10
4	Moduły kształcenia językowego	100	0	60	40	80	0	40	40
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	266	80	186	0	122	44	78	0
7	Moduły praktyk kierunkowych	240	2	10	228	240	2	10	228
8	Moduły praktyk specjalnościowych	240	2	10	228	240	2	10	228

2. Stosowane metody dydaktyczne oraz sposoby weryfikacji i oceny efektów uczenia się osiąganych przez studenta w trakcie całego cyklu kształcenia

Karty przedmiotów definiują przedmiotowe efekty uczenia się, które należy osiągnąć, aby program studiów został zrealizowany. Efekty uczenia się dla poszczególnych przedmiotów są mierzalne i weryfikowane między innymi poprzez testy, prace projektowe, raporty z ćwiczeń laboratoryjnych, analizy studiów przypadków lub symulacji, kolokwia ustne i egzaminy. Studenci otrzymują wsparcie edukacyjne nie tylko dzięki rzetelnemu przygotowaniu zajęć przez wykładowców, ale również poprzez realizowany w uczelni program tutoringu akademickiego oraz projekty edukacyjne, jakie mogą przeprowadzić w ramach działającej na uczelni Akademii Umiejętności. Nauczyciele oraz tutorzy są dostępni poza wykładami, ćwiczeniami i zajęciami z tutorem, w trakcie cotygodniowych konsultacji, pomagając rozwiązać indywidualne problemy poszczególnych studentów.

Uniwersytet DSW Ideis dysponuje odpowiednią infrastrukturą, także informatyczną, wspierającą proces dydaktyczny. Służy temu również platforma MS Teams, która prowadzącemu zajęcia pozwala umieszczać na niej wszelkie materiały zapisane w formie elektronicznej, prowadzić asynchroniczne panele dyskusyjne na zadane tematy. Platforma kształcenia zdalnego MS Teams służy do zamieszczania materiałów dydaktycznych dla studentów. Standardem jest zamieszczenie kart przedmiotu, które zawierają podstawowe informacje o prowadzonym przedmiocie, takie jak wymiar godzin, realizowane zagadnienia czy też wykaz literatury. Każdy pracownik ma możliwość udostępniania studentom, w ramach prowadzonych zajęć, dodatkowych materiałów do wykładów i ćwiczeń odbywających się w siedzibie Uczelni, zarówno materiałów podstawowych, jak i poszerzających wiedzę. Zaproponowany program studiów na kierunku zarządzanie cyberbezpieczeństwem został opracowany w oparciu o metody dydaktyczne, które sprzyjają osiąganiu założonych efektów uczenia się. Dotyczy to zarówno metod podających (wykład interaktywny), problemowych (dyskusje problemowe, uczenie się problemowe, case study), eksponujących (prezentacja), praktycznych, w tym: symulacji, superwizji, gier, symulacji grupowych, Assessment Centre, gier kierowniczych, opracowania studium przypadku lub metody projektowej. Wybór metod podyktowany jest potrzebą prowadzenia procesu kształcenia studentów w taki sposób, aby stwarzał warunki do zaangażowanego i aktywnego ich udziału w pracy na zajęciach.

Osiągane efekty uczenia się w zakresie wiedzy zwykle weryfikowane są poprzez egzaminy, kolokwia, quizy, testy oraz projekty. Natomiast umiejętności zwykle weryfikowane są poprzez ocenę aktywności na zajęciach, merytoryczny udział w dyskusji, projekty indywidualne lub grupowe, raporty z ćwiczeń laboratoryjnych, symulacji, opracowania studium przypadków. Osiąganie przez studenta efektów uczenia się w zakresie kompetencji społecznych zwykle weryfikowane jest poprzez ocenę merytorycznej aktywności na zajęciach, ocenę pracy zespołowej nad projektem, obserwację, ocenę prezentacji wyników projektu lub opracowania grupowego raportu z zadań laboratoryjnych.

W ramach każdego z narzędzi nauczyciel akademicki ustala kryteria i sposób oceny tego, czy dany efekt uczenia się został osiągnięty przez studenta. W trakcie interaktywnych wykładów, często wspartych prezentacjami multimedialnymi, student ma możliwość zdobycia nowej, specjalistycznej wiedzy i spotkania się z przedstawicielami dziedziny nauk społecznych, specjalistów z zakresu zarządzania cyberbezpieczeństwem, bezpieczeństwa informacji i zgodności regulacyjnej. Spotkania w ramach wykładów, jak również indywidualnych spotkań z nauczycielami akademickimi w czasie ich konsultacji, dają szansę na rozwój profesjonalnych umiejętności niezbędnych w codziennej praktyce zawodowej. W procesie kształcenia studentów wykorzystane zostaną również metody praktyczne. W szczególności dotyczy to metody projektów (warsztatów), kształtującej i rozwijającej umiejętności, nawyki i sprawności o charakterze praktycznym, niezbędne przy realizowaniu konkretnych działań praktycznych w przestrzeni biznesowej. Kolejne przewidziane metody dydaktyczne, tj.: metody aktywizujące, ćwiczenia przedmiotowe, służą kształtowaniu umiejętności twórczego wykorzystania wiedzy w samodzielnym projektowaniu i realizowaniu indywidualnych projektów. Sprzyja temu praca w małych grupach (praca w zespole), polegająca na wykonaniu konkretnych zadań zleconych przez wykładowcę/trenera, która aktywizuje do działania, kształtuje umiejętności organizacyjne, przywódcze i kompetencje interpersonalne.

3. Wykaz przedmiotów do wyboru pozwalających na stwierdzenie, że program studiów umożliwia studentowi wybór modułów w wymiarze nie mniejszym niż 30% punktów ECTS

Program studiów umożliwia studentowi wybór modułów kształcenia, do których przypisuje się punkty ECTS w wymiarze nie mniejszym niż 30% liczby punktów ECTS. Do modułów wybieralnych należą moduły wskazane poniżej.

Specjalność	Liczba punktów ECTS	
	Studia stacjonarne	Studia niestacjonarne
Managing diverse teams and conflict resolution/ Management vielfältiger Teams und Konfliktlösung	4	4
Moduły kształcenia wybieralnego / specjalnościowego:	21	21
Zarządzanie Bezpieczeństwem Sztucznej Inteligencji		
Zarządzanie Audytami i Jakością w Bezpieczeństwie Informacji		
Moduły praktyk kierunkowych	10	10
Warsztat kompetencji językowych	6	6
Łącznie	**41**	**41**

Informacja o proponowanych modułach kształcenia wybieralnego / specjalnościowego oferowanych w danym cyklu kształcenia:

Zarządzanie Bezpieczeństwem Sztucznej Inteligencji

Specjalność Zarządzanie Bezpieczeństwem Sztucznej Inteligencji koncentruje się na zarządzaniu ryzykiem, zgodnością prawną i etyką w kontekście projektowania, trenowania, wdrażania i nadzoru systemów sztucznej inteligencji. Program kształtuje kompetencje w zakresie wdrażania norm i standardów międzynarodowych (ISO/IEC 27001, ISO/IEC 42001, ISO 31000). Absolwent rozumie pełny cykl życia systemów AI oraz ich wpływ na bezpieczeństwo danych i procesów organizacyjnych.

Absolwent specjalności Zarządzanie Bezpieczeństwem Sztucznej Inteligencji w czasie studiów zdobędzie wiedzę i umiejętności w zakresie:

- analizy zagrożeń wynikających z automatyzacji procesów decyzyjnych oraz opracowywania polityk bezpieczeństwa AI;
- oceny ryzyk technologicznych, prawnych i etycznych związanych z systemami AI;
- procesów oceny zgodności systemów AI z wymaganiami unijnymi (AI Act, GDPR, NIS2);
- budowania dokumentacji, mechanizmów nadzoru i raportowania wymaganych przez organy nadzoru;
- współpracy z zespołami technicznymi, prawnymi i biznesowymi w zakresie zarządzania ryzykiem AI.

Specjalność przygotowuje absolwentów do podjęcia pracy na takich stanowiskach jak:

Specjalista ds. zarządzania bezpieczeństwem AI (AI Security Governance Specialist),
Ekspert ds. ryzyka i zgodności AI (AI Risk and Compliance Officer),
Menedżer ds. zgodności z Aktem o Sztucznej Inteligencji (AI Act Compliance Manager),
Konsultant ds. etyki i ryzyka w AI (AI Ethics & Risk Consultant),
Doradca strategii bezpieczeństwa sztucznej inteligencji (AI Cybersecurity Advisor).

Zarządzanie Audytami i Jakością w Bezpieczeństwie Informacji

Specjalność Zarządzanie Audytami i Jakością w Bezpieczeństwie Informacji rozwija kompetencje menedżerskie i analityczne w zakresie prowadzenia audytów bezpieczeństwa informacji, zarządzania ryzykiem, zgodnością prawną (compliance) oraz jakością procesów w środowisku cyfrowym. Program łączy wiedzę z zakresu ISO/IEC 27001, ISO 9001, ISO 22301 oraz ISO 31000.

Absolwent w czasie studiów zdobędzie wiedzę i umiejętności z zakresu:

- metodyki audytu zgodności i oceny dojrzałości procesów bezpieczeństwa;
- projektowania systemów monitorowania i raportowania bezpieczeństwa informacji (KPI, KRI);
- współpracy z organami nadzoru i certyfikującymi w zakresie NIS2, RODO, DORA;
- koordynowania prac zespołów audytowych i przygotowywania organizacji do certyfikacji ISO 27001.

Specjalność przygotowuje absolwentów do podjęcia pracy na takich stanowiskach jak:

Audytor bezpieczeństwa informacji (Information Security Auditor),
Menedżer ds. jakości i zgodności (Quality & Compliance Manager),
Kierownik zespołu ds. audytu IT lub bezpieczeństwa (IT/IS Audit Team Lead),
Inspektor ochrony danych (DPO -Data Protection Officer),
Specjalista ds. zgodności regulacyjnej (Compliance Specialist).

4. Wymiar, zasady i formy odbywania praktyk zawodowych

W programie kształcenia dla kierunku zarządzanie cyberbezpieczeństwem o profilu praktycznym na studiach drugiego stopnia przewidziano praktyki w wymiarze 480 godzin, co odpowiada 19 punktom ECTS. Praktyki będą realizowane w następujący sposób:

- II semestr -4 tygodnie praktyki zawodowej ogólnej (160 h), co odpowiada 6 punktom ECTS;
- III semestr -8 tygodni praktyki zawodowej kierunkowej (320 h), co odpowiada 13 punktom ECTS.

Wybór miejsca i procedura kierowania na praktyki

Przy wyborze miejsca odbywania praktyki uwzględnia się, poza studiowanym kierunkiem, predyspozycje studenta, jego preferencje oraz możliwości Uczelni. Biuro Karier i Praktyk stara się zapewnić studentom możliwość odbywania praktyki w miejscu zamieszkania.

Studentki i studenci mogą odbyć praktyki w następujących miejscach:

- działy bezpieczeństwa informacji, compliance i zarządzania ryzykiem w przedsiębiorstwach różnych sektorów;

- urzędy regulacyjne, organy nadzoru i instytucje certyfikujące (np. UKE, CERT, KNF, UODO);
- firmy konsultingowe specjalizujące się w cyberbezpieczeństwie i zarządzaniu ryzykiem IT;
- instytucje finansowe i banki z wyodrębnionymi działami bezpieczeństwa cyfrowego;
- przedsiębiorstwa technologiczne i dostawcy rozwiązań cybersecurity;
- administracja publiczna i jednostki samorządu terytorialnego;
- instytucje doradcze i think-tanki zajmujące się strategicznym bezpieczeństwem (np. Defence Institute).

Studentka/Student dokonuje wyboru miejsca praktyki z bazy pracodawców Biura Karier i Praktyk dostępnej na stronie internetowej Uczelni lub ma możliwość samodzielnego zgłoszenia propozycji Instytucji Przyjmującej na praktykę Uczelnianemu Opiekunowi Praktyk. W takim przypadku Uczelniany Opiekun Praktyk weryfikuje wskazanego pracodawcę pod kątem możliwości realizacji efektów uczenia się przewidzianych dla praktyki. Uczelniany Opiekun Praktyk może zgłosić Studentce/Studentowi propozycję dodania Pracodawcy do bazy pracodawców na *Formularzu zgłoszenia pracodawcy* (załącznik nr 2 do Zarządzenia nr 6/2023 Dziekana WSS). Po akceptacji miejsca odbywania praktyk przez Uczelnianego Opiekuna Praktyka Student odbiera komplet dokumentów niezbędnych do realizacji praktyk z Biura Karier i Praktyk:

a. *Skierowanie na praktykę* (załącznik nr 3 część B do Zarządzenia nr 6/2023 Dziekana WSS),
b. *Potwierdzenie przyjęcia na praktykę* (załącznik nr 3 część A do Zarządzenia nr 6/2023 Dziekana WSS).

Instytucja Przyjmująca na praktykę (wybrany pracodawca) rozpatruje *Skierowanie na praktykę* i zwraca studentowi wypełnione i podpisane *Potwierdzenie przyjęcia na praktykę* wraz z podpisaną *Umową o praktyki.* Następnie Studentka/Student przekazuje do Biura Karier i Praktyk (przed terminem rozpoczęcia praktyki) wypełnione *Potwierdzenie przyjęcia na praktykę*. Biuro Karier i Praktyk odnotowuje w *Rejestrze praktyk na kierunku* wpłynięcie dokumentacji praktyk od Studenta oraz kontaktuje się z praktykodawcą w celu podpisania umowy oraz porozumienia.

Osoby odpowiedzialne za organizację i przebieg praktyk studenckich oraz ich zadania w obszarze praktyk:

- ze strony jednostki organizacyjnej przyjmującej Studentkę/Studenta: Opiekun praktyk w Placówce, powołany przez Dyrektora Placówki, w której odbywana jest praktyka -zgodnie z *Programem i Regulaminem praktyk* (Załącznik nr 1 do Zarządzenia nr 6/2023 Dziekana WSS);
- ze strony Uniwersytetu Dolnośląskiego DSW:
    - **Dyrektor Biura Karier i Praktyk** -odpowiedzialny za organizację pracy Działu;
    - **Pracownicy Biura Karier i Praktyk** -odpowiedzialni za:
        - przygotowywanie dokumentacji praktyk niezbędnej do przeprowadzenia przez Uczelnianych Opiekunów Praktyk zajęć z wprowadzenia do praktyk na poszczególnych kierunkach,
        - przygotowywanie umów o praktykę,
        - rozliczanie umów o praktykę,
        - stworzenie bazy Instytucji Przyjmujących na praktykę dla poszczególnych kierunków,
        - prowadzenie rejestru praktyk dla kierunków i form studiów,
        - współpracę z opiekunami praktyk w miejscu odbywania praktyk,
        - przeprowadzanie hospitacji w miejscu realizacji praktyk (min. 10% miejsc praktyk wskazanych dla kierunku studiów),
        - prowadzenie Rejestru hospitacji praktyk prowadzonych na kierunkach,
        - przygotowanie raportu z realizacji praktyk w danym roku akademickim, który przekazywany jest Dziekanowi Wydziału oraz Wydziałowej Komisji ds. Oceny Jakości Kształcenia,
        - wspomaganie karier edukacyjno-zawodowych studentów i absolwentów Uczelni (pozyskiwanie i upowszechnianie aktualnych ofert praktyk, staży, zatrudnienia, wolontariatu dla studentów oraz upowszechnianie informacji i doradztwo w zakresie

konkursów, stypendiów, pozaformalnych ofert edukacyjnych adresowanych do studentów oraz absolwentów szkół wyższych; wspieranie studentów DSW w trudnych sytuacjach życiowych, psychologicznych i zawodowych poprzez świadczenie na ich rzecz usług w zakresie całożyciowego poradnictwa kariery),

- wspieranie procesu kształcenia studentów i doktorantów z niepełnosprawnością (określanie potrzeb studentów i doktorantów w zakresie wsparcia edukacyjnego; realizowanie wsparcia dla studentów i doktorantów z niepełnosprawnością; świadczenie usług w zakresie poradnictwa edukacyjno-zawodowego dla studentów i doktorantów z niepełnosprawnością);

- **Uczelniany Opiekun praktyk studenckich** -nauczyciel akademicki prowadzący przedmiot z modułu praktyk, jest odpowiedzialny za:
  - wprowadzenie studentów do praktyk,
  - zapoznanie studentów z celem i programem praktyk oraz zasadami jej odbywania i zaliczania,
  - rozpatrywanie wniosków o włączeniu podmiotu do bazy praktyk w danym roku akademickim,
  - rozstrzyganie wspólnie ze studentem oraz Instytucją Przyjmującą na praktyki spraw związanych z organizacją i przebiegiem praktyki oraz powstałymi sporami,
  - formalne sprawdzenie *Dziennika praktyk*,
  - opiniowanie podań w sprawie zaliczania na rzecz praktyki innej aktywności zawodowej, staży, praktyk studenta, o ile aktywności te są udokumentowane i umożliwiają osiągnięcie zakładanych efektów uczenia się dla kierunku studiów,
  - przeprowadzanie wyrywkowych kontroli i hospitacji w czasie trwania praktyki Studenta w celu zaznajomienia się z opinią Opiekuna Praktyk w Instytucji Przyjmującej na praktykę na temat przebiegu praktyki i postawy praktykanta,
  - uzupełnianie wspólnego rejestru praktyk dla poszczególnych kierunków i form studiów udostępnionego przez Biuro Karier i Praktyk;
- **Menedżer Kierunku** -odpowiedzialny za koncepcję praktyk, plan studiów i wynikającą z niego organizację praktyk studenckich, obsady nauczycieli akademickich, w tym opiekunów praktyk z ramienia Uniwersytetu;
- **Pełnomocnik Dziekana ds. praktyk studenckich** -nauczyciel akademicki odpowiedzialny za opracowanie założeń merytorycznych do odbywania praktyk studenckich.

III. Dodatkowe dokumenty do programu studiów

1. System ECTS

Zasady przypisywania punktów ECTS do przedmiotów zostały określone zgodnie z ustawą Prawo o Szkolnictwie Wyższym i Nauce z 20 lipca 2018 r. (ze zmianami) i aktami wykonawczymi.

Liczbę punktów ECTS przypisaną do poszczególnych przedmiotów określonych w programie studiów zatwierdza Senat uczelni, podejmując stosowną uchwałę w sprawie przyjęcia planów i programów studiów na dany rok akademicki. W przypisywaniu punktów poszczególnym przedmiotom kierowano się zasadą, iż wymiar punktów musi uwzględniać rzeczywisty nakład pracy studenta. Przyjęto, że 1 punkt ECTS odpowiada około 25 godzinom pracy studenta.

Wartość punktów ECTS dla danego przedmiotu odzwierciedla średni nakład pracy studenta niezbędny do uzyskania zakładanych efektów uczenia się. Nakład ten jest sumą godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów (godziny kontaktowe) oraz godzin

pracy samodzielnej studenta. Zgodnie z tą zasadą przydzielono punkty ECTS na poszczególne formy procesu dydaktycznego składające się na realizacje efektów uczenia się danego przedmiotu, takich jak wykłady, ćwiczenia, konwersatorium, lektoraty, seminaria, projekty, e-learning i praca własna studenta. Uwzględniono również punkty ECTS realizowane przez bezpośredni kontakt nauczyciela akademickiego w formie egzaminów, zaliczeń, konsultacji oraz prac dodatkowych wykonywanych przez studentów pod nadzorem nauczyciela akademickiego. Nakład pracy własnej studenta przypadającej na dany przedmiot (a w konsekwencji liczba punktów ECTS za pracę własną studenta) jest wypadkową szeregu czynników istotnych dla osiągnięcia zakładanych efektów uczenia się i jest wynikiem analizy stopnia trudności związanego z zakładanymi efektami uczenia się przypisanymi do przedmiotu, a także konsultacji z wykładowcami prowadzącymi poszczególne przedmioty. Dla określenia średniego nakładu pracy własnej studenta w danym przedmiocie brany jest także pod uwagę kontekst, w jakim ten przedmiot występuje w programie studiów -czy zdobycie efektów uczenia się przypisanych do przedmiotu wymaga wcześniejszego zaliczenia innych przedmiotów lub posiadania innego zasobu wiedzy lub umiejętności.

Przypisane w ten sposób punkty ECTS do przedmiotów są takie same w przypadku studiów stacjonarnych i niestacjonarnych, ale inne są składniki, z jakich te punkty zostały uzyskane. W ramach studiów niestacjonarnych zostało zaplanowane mniej godzin kontaktowych, więc aby uzyskać takie same efekty uczenia się jak na studiach stacjonarnych, potrzebna jest większa ilość pracy własnej studenta.

Projektując system przypisywania punktów ECTS, uwzględniono doświadczenia uczelni zagranicznych, z którymi współpracuje Uczelnia. Stosowanie systemu przypisywania punktów ECTS w sposób zbliżony do uczelni partnerskich ułatwia mobilność studentów w Europejskim Obszarze Szkolnictwa Wyższego.

2. Treści modułów

Nazwa modułu	Treści modułu
Moduły kształcenia podstawowego	Współczesne wyzwania zarządzania; Współczesne zagrożenia bezpieczeństwa; Matematyka dyskretna; Etyka i psychologia cyberbezpieczeństwa; Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO); Szkolenie wstępne z zakresu BHP
Moduły kształcenia kierunkowego	Kontekst organizacji i zarządzanie interesariuszami; Kategorie cyberzagrożeń i podatności; Kryptografia i blockchain; Zarządzanie kryzysowe; Komunikacja społeczna w sytuacjach zagrożeń cyfrowych; Zarządzanie różnorodnymi zespołami i rozwiązywanie konfliktów; Architektura Systemu Zarządzania Bezpieczeństwem Informacji; Metodyki zarządzania projektami; Zarządzanie zmianą i transformacją cyfrową; Zarządzanie odpornością organizacji i ciągłością działania; Technologiczne trendy i wpływ na organizacje
Moduły przygotowania pracy dyplomowej	Metody i techniki badań społecznych z elementami AI; Seminarium magisterskie I; Seminarium magisterskie II
Moduły kształcenia językowego	Warsztaty kompetencji językowych (j. angielski, j. niemiecki);
Moduły praktyk kierunkowych	Praktyka kierunkowa 1 -realizowana w instytucji zgodnie z regulaminem i programem praktyk na kierunku
Moduły kształcenia wybieralnego (kształcenie w zakresie) **Zarządzanie Bezpieczeństwem Sztucznej Inteligencji**	Bezpieczeństwo danych, prywatność i bias w AI; Normy i uwarunkowania prawne AI; Modele implementacji sztucznej inteligencji; AI w systemach bezpieczeństwa, infrastrukturze krytycznej i IoT; Nadzór nad AI i zarządzanie ryzykiem; Automatyzacja i integracja AI w systemach bezpieczeństwa;
Moduły kształcenia wybieralnego (kształcenie w zakresie) **Zarządzanie Audytami i Jakością w Bezpieczeństwie Informacji**	Polityka bezpieczeństwa i zgodność w dobie regulacji cyfrowych; Strategiczne zarządzanie incydentami -aspekty techniczne i psychologiczne; Audyt bezpieczeństwa informacji i systemów; Nadzór nad cyberbezpieczeństwem w organizacji; Budowanie i wdrażanie

	strategii bezpieczeństwa organizacji; Narzędzia wspierające zgodność z przepisami;

3. Załączniki do programu studiów

Załącznik 1. Plany studiów
Załącznik 2. Macierz efektów uczenia się
Załącznik 3. Sumaryczne wskaźniki ECTS
Załącznik 4. Treści programowe przypisane do zajęć

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: *Zarządzanie cyberbezpieczeństwem*
Stopień kształcenia: studia drugiego stopnia
Forma studiów: niestacjonarne
Profil: praktyczny
dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 4 semestry
Obowiązuje od roku akademickiego: 2026/2027

Moduły kształcenia podstawowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N2-00-WSPWYZWZA-1	Współczesne wyzwania zarządzania	E	5	26	12	14	0	12	14										
2	N2-00-WSPZAGBEZ-1	Współczesne zagrożenia bezpieczeństwa	O	4	24	0	14	10		14	10									
3	N2-00-MATDYSKRE-1	Matematyka dyskretna	O	4	20	0	20	0		20										
4	N2-00-ETPSYCHCYB-1	Etyka i psychologia cyberbezpieczeństwa	O	3	16	0	16	0		16										
5	N2-00-REGLPRAWC-1	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	O	3	16	16	0	0	16											
6	N2-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4			4									
		RAZEM:		**19**	**106**	**28**	**64**	**14**	**28**	**64**	**14**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Moduły kształcenia kierunkowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N2-00-KONORGINT-1	Kontekst organizacji i zarządzanie interesariuszami	O	3	16	0	16	0		16										
2	N2-00-KATCYBPOD-2	Kategorie cyberzagrożeń i podatności	O	3	16	16	0	0				16								
3	N2-00-KRYPTBLCK-2	Kryptografia i blockchain	O	4	24	12	12	0				12	12							
4	N2-00-ZARRYZYKR-2	Zarządzanie kryzysowe	O	3	16	0	16	0					16							
5	N2-00-KOMSPSYTZ-4	Komunikacja społeczna w sytuacjach zagrożeń cyfrowych	O	3	16	0	16	0											16	
6	N2-00-ZARZROZKO-4	Managing Diverse Teams and Conflict Resolution / Management vielfältiger Teams und Konfliktlösung	O	4	24	12	12	0										12	12	
7	N2-00-ARCHITSZBI-3	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	E	5	36	12	14	10							12	14	10			
8	N2-00-METZARPRJ-1	Metodyki zarządzania projektami	O	3	16	0	16	0		16										
9	N2-00-ZARZMICTR-3	Zarządzanie zmianą i transformacją cyfrową	O	4	24	0	14	10								14	10			
10	N2-00-ZARODPCIO-4	Zarządzanie odpornością organizacji i ciągłością działania	O	5	36	12	14	10										12	14	10
11	N2-00-TECHTRENOR-2	Technologiczne trendy i wpływ na organizacje	O	5	26	12	14	0				12	14							
		RAZEM:		**42**	**250**	**76**	**144**	**30**	**0**	**32**	**0**	**40**	**42**	**0**	**12**	**28**	**20**	**24**	**42**	**10**

Moduły przygotowania pracy dyplomowej

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N2-00-METTECBAD-2	Metody i techniki badań społecznych z elementami AI	O	4	24	0	14	10					14	10						
2	N2-00-SEMMGR1-3	Seminarium magisterskie I	O	4	18	0	18	0								18				
3	N2-00-SEMMGR2-4	Seminarium magisterskie II	O	5	20	0	20	0											20	
		RAZEM:		**13**	**62**	**0**	**52**	**10**	**0**	**0**	**0**	**0**	**14**	**10**	**0**	**18**	**0**	**0**	**20**	**0**

Moduły kształcenia językowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N2-00-WAJEZ1-3	Warsztaty kompetencji językowych I (j. angielski, j. niemiecki)	O	3	40	0	20	20								20	20			
2	N2-00-WAJEZ2-4	Warsztaty kompetencji językowych II (j. angielski, j. niemiecki)	E	3	40	0	20	20											20	20
		RAZEM:		**6**	**80**	**0**	**40**	**40**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**20**	**20**	**0**	**20**	**20**

Moduły praktyk kierunkowych

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N2-00-PRAKTYKA1-2	Praktyka kierunkowa 1	ZAL	9	240	2	10	228				2	10	228						
					0	0	0	0												
		RAZEM:		**9**	**240**	**2**	**10**	**228**	**0**	**0**	**0**	**2**	**10**	**228**	**0**	**0**	**0**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr											
						sem. 1			sem. 2			sem. 3			sem 4		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	106	28	64	14	28	64	14	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	250	76	144	30	0	32	0	40	42	0	12	28	20	24	42	10
3	Moduły przygotowania pracy dyplomowej	62	0	52	10	0	0	0	0	14	10	0	18	0	0	20	0
4	Moduły kształcenia językowego	80	0	40	40	0	0	0	0	0	0	0	20	20	0	20	20
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Razem bez modułu praktyk kierunkowych:	**498**	**104**	**300**	**94**	**28**	**96**	**14**	**40**	**56**	**10**	**12**	**66**	**40**	**24**	**82**	**30**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
6	Moduły praktyk kierunkowych	240	2	10	228	0	0	0	2	10	228	0	0	0	0	0	0
	RAZEM z modułem praktyk kierunkowych:	**738**				**138**			**346**			**118**			**136**		

Punkty ECTS

Lp.		Liczba punktów	Semestr			
			sem. 1	sem. 2	sem. 3	sem 4
1	Moduły kształcenia podstawowego	19	19	0	0	0
2	Moduły kształcenia kierunkowego	42	6	15	9	12
3	Moduły przygotowania pracy dyplomowej	13	0	4	4	5
4	Moduły kształcenia językowego	6	0	0	3	3
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0
6	Moduły praktyk kierunkowych	9	0	9	0	0
	RAZEM:	**89**	**25**	**28**	**16**	**20**
	Moduł kształcenia specjalnościowego:	*31*	*5*	*2*	*14*	*10*
	OGÓŁEM:	**120**	**30**	**30**	**30**	**30**
	Dopuszczalny deficyt punktowy po semetrze:		-5	-5	-5	-5

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Zarządzanie bezpieczeństwem sztucznej inteligencji*
Stopień kształcenia: studia drugiego stopnia **Czas trwania:** 4 semestry
Forma studiów: niestacjonarne **Obowiązuje od roku akademickiego:** 2026/2027
Profil: praktyczny

Moduły kształcenia specjalnościowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N2-00-BEZDDANAI-2	Bezpieczeństwo danych, prywatność i bias w AI	O	3	16	0	16	0					16							
2	N2-00-NORPRWAI-2	Normy i uwarunkowania prawne AI	O	4	20	20	0	0				20								
3	N2-00-MODIMPAI-4	Modele implementacji sztucznej inteligencji	O	5	32	12	20	0										12	20	
4	N2-00-AISYBINFR-3	AI w systemach bezpieczeństwa, infrastrukturze krytycznej i IOT	O	5	26	12	14	0							12	14				
5	N2-00-AIGOVRISK-3	Nadzór nad AI i zarządzanie ryzykiem	O	2	14	0	14	0								14				
6	N2-00-AUTOAISEC-4	Automatyzacja i integracja AI w systemach bezpieczeństwa	O	2	14	0	14	0											14	
RAZEM:				**21**	**122**	**44**	**78**	**0**	**0**	**0**	**0**	**20**	**16**	**0**	**12**	**28**	**0**	**12**	**34**	**0**

Moduły praktyk specjalnościowych

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228							2	10	228			
2					0	0	0	0												
RAZEM:				**10**	**240**	**2**	**10**	**228**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**228**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr											
						sem. 1			sem. 2			sem. 3			sem 4		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	106	28	64	14	28	64	14	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	250	76	144	30	0	32	0	40	42	0	12	28	20	24	42	10
3	Moduły przygotowania pracy dyplomowej	62	0	52	10	0	0	0	0	14	10	0	18	0	0	20	0
4	Moduły kształcenia językowego	80	0	40	40	0	0	0	0	0	0	0	20	20	0	20	20
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	122	44	78	0	0	0	0	20	16	0	12	28	0	12	34	0
	Ogółem bez praktyk	**620**	**148**	**378**	**94**	**28**	**96**	**14**	**60**	**72**	**10**	**24**	**94**	**40**	**36**	**116**	**30**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	240	2	10	228	0	0	0	2	10	228	0	0	0	0	0	0
	Ogółem praktyki	**480**	**4**	**20**	**456**	**0**	**0**	**0**	**2**	**10**	**228**	**2**	**10**	**228**	**0**	**0**	**0**
	OGÓŁEM:	**1100**				**138**			**382**			**398**			**182**		

Punkty ECTS

Lp.		Liczba punktów	Semestr			
			sem. 1	sem. 2	sem. 3	sem 4
1	Moduły kształcenia podstawowego	19	19	0	0	0
2	Moduły kształcenia kierunkowego	42	6	15	9	12
3	Moduły przygotowania pracy dyplomowej	13	0	4	4	5
4	Moduły kształcenia językowego	6	0	0	3	3
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	21	0	7	7	7
	Ogółem bez praktyk	**101**	**25**	**26**	**23**	**27**
7	Moduły praktyk kierunkowych	9	0	9	0	0
8	Moduły praktyk specjalnościowych	10	0	0	10	0
	Ogółem praktyki	**19**	**0**	**9**	**10**	**0**
	OGÓŁEM:	**120**	**25**	**35**	**33**	**27**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**550**
Liczba godzin zajęć e-learningowych i projektów	**94**
Liczba godzin praktyk w Instytucji	**456**
Łączna liczba godzin w programie	**1100**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Zarządzanie audytami i jakością*
Stopień kształcenia: studia drugiego stopnia **Czas trwania:** 4 semestry
Forma studiów: niestacjonarne **Obowiązuje od roku akademickiego:** 2026/2027
Profil: praktyczny

Moduły kształcenia specjalnościowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N2-00-POLBEZGOD-2	Polityka bezpieczeństwa i zgodność w dobie regulacji cyfrowych	O	3	16	0	16	0					16							
2	N2-00-STRZARINC-2	Strategiczne zarządzanie incydentami – aspekty techniczne i psychologiczne	O	4	20	20	0	0				20								
3	N2-00-AUDYBEZIS-4	Audyt bezpieczeństwa informacji i systemów	O	5	32	12	20	0										12	20	
4	N2-00-CYBERGOV-3	Nadzór nad cyberbezpieczeństwem w organizacji	O	5	26	12	14	0							12	14				
5	N2-00-BUDWSTRB-3	Budowanie i wdrażanie strategii bezpieczeństwa organizacji	O	2	14	0	14	0								14				
6	N2-00-NOWNCOMP-4	Narzędzia wspierające zgodność z przepisami	O	2	14	0	14	0											14	
RAZEM:				**21**	**122**	**44**	**78**	**0**	**0**	**0**	**0**	**20**	**16**	**0**	**12**	**28**	**0**	**12**	**34**	**0**

Moduły praktyk specjalnościowych

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228							2	10	228			
2					0	0	0	0												
RAZEM:				**10**	**240**	**2**	**10**	**228**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**228**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr											
						sem. 1			sem. 2			sem. 3			sem 4		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	106	28	64	14	28	64	14	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	250	76	144	30	0	32	0	40	42	0	12	28	20	24	42	10
3	Moduły przygotowania pracy dyplomowej	62	0	52	10	0	0	0	0	14	10	0	18	0	0	20	0
4	Moduły kształcenia językowego	80	0	40	40	0	0	0	0	0	0	0	20	20	0	20	20
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	122	44	78	0	0	0	0	20	16	0	12	28	0	12	34	0
	Ogółem bez praktyk	**620**	**148**	**378**	**94**	**28**	**96**	**14**	**60**	**72**	**10**	**24**	**94**	**40**	**36**	**116**	**30**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	240	2	10	228	0	0	0	2	10	228	0	0	0	0	0	0
8	Moduły praktyk specjalnościowych	240	2	10	228	0	0	0	0	0	0	2	10	228	0	0	0
	Ogółem praktyki	**480**	**4**	**20**	**456**	**0**	**0**	**0**	**2**	**10**	**228**	**2**	**10**	**228**	**0**	**0**	**0**
	OGÓŁEM:	**1100**				**138**			**382**			**398**			**182**		

Punkty ECTS

Lp.		Liczba punktów	Semestr			
			sem. 1	sem. 2	sem. 3	sem 4
1	Moduły kształcenia podstawowego	19	19	0	0	0
2	Moduły kształcenia kierunkowego	42	6	15	9	12
3	Moduły przygotowania pracy dyplomowej	13	0	4	4	5
4	Moduły kształcenia językowego	6	0	0	3	3
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	21	0	7	7	7
	Ogółem bez praktyk	**101**	**25**	**26**	**23**	**27**
7	Moduły praktyk kierunkowych	9	0	9	0	0
8	Moduły praktyk specjalnościowych	10	0	0	10	0
	Ogółem praktyki	**19**	**0**	**9**	**10**	**0**
	OGÓŁEM:	**120**	**25**	**35**	**33**	**27**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**550**
Liczba godzin zajęć e-learningowych i projektów	**94**
Liczba godzin praktyk w Instytucji	**456**
Łączna liczba godzin w programie	**1100**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: *Zarządzanie cyberbezpieczeństwem*
Stopień kształcenia: studia drugiego stopnia
Forma studiów: stacjonarne
Profil: praktyczny
dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 4 semestry
Obowiązuje od roku akademickiego: 2026/2027

Moduły kształcenia podstawowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S2-00-WSPWYZWZA-1	Współczesne wyzwania zarządzania	E	5	70	30	40	0	30	40										
2	S2-00-WSPZAGBEZ-1	Współczesne zagrożenia bezpieczeństwa	O	4	50	20	20	10	20	20	10									
3	S2-00-MATDYSKRE-1	Matematyka dyskretna	O	4	50	20	30	0	20	30										
4	S2-00-ETPSYCHCYB-1	Etyka i psychologia cyberbezpieczeństwa	O	3	36	0	36	0		36										
5	S2-00-REGLPRAWC-1	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	O	3	36	36	0	0	36											
6	S2-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4			4									
		RAZEM:		**19**	**246**	**106**	**126**	**14**	**106**	**126**	**14**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Moduły kształcenia kierunkowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S2-00-KONORGINT-1	Kontekst organizacji i zarządzanie interesariuszami	O	3	36	0	36	0		36										
2	S2-00-KATCYBPOD-2	Kategorie cyberzagrożeń i podatności	O	3	36	36	0	0				36								
3	S2-00-KRYPTBLCK-2	Kryptografia i blockchain	O	4	50	20	30	0				20	30							
4	S2-00-ZARRYZYKR-2	Zarządzanie kryzysowe	O	3	36	0	36	0					36							
5	S2-00-KOMSPSYTZ-4	Komunikacja społeczna w sytuacjach zagrożeń cyfrowych	O	3	36	0	36	0											36	
6	S2-00-ZARZROZKO-4	Managing Diverse Teams and Conflict Resolution / Management vielfältiger Teams und Konfliktlösung	O	4	50	20	30	0										20	30	
7	S2-00-ARCHITSZBI-3	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	E	5	80	30	40	10							30	40	10			
8	S2-00-METZARPRJ-1	Metodyki zarządzania projektami	O	3	36	0	36	0		36										
9	S2-00-ZARZMICTR-3	Zarządzanie zmianą i transformacją cyfrową	O	4	40	0	30	10								30	10			
10	S2-00-ZARODPCIO-4	Zarządzanie odpornością organizacji i ciągłością działania	O	5	80	30	40	10										30	40	10
11	S2-00-TECHTRENOR-2	Technologiczne trendy i wpływ na organizacje	O	5	70	30	40	0				30	40							
		RAZEM:		**42**	**550**	**166**	**354**	**30**	**0**	**72**	**0**	**86**	**106**	**0**	**30**	**70**	**20**	**50**	**106**	**10**

Moduły przygotowania pracy dyplomowej

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S2-00-METTECBAD-2	Metody i techniki badań społecznych z elementami AI	O	4	40	0	30	10					30	10						
2	S2-00-SEMMGR1-3	Seminarium magisterskie I	O	4	32	0	32	0								32				
3	S2-00-SEMMGR2-4	Seminarium magisterskie II	O	5	36	0	36	0											36	
		RAZEM:		**13**	**108**	**0**	**98**	**10**	**0**	**0**	**0**	**0**	**30**	**10**	**0**	**32**	**0**	**0**	**36**	**0**

Moduły kształcenia językowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S2-00-WAJEZ1-3	Warsztaty kompetencji językowych I (j. angielski, j. niemiecki)	O	3	50	0	30	20								30	20			
2	S2-00-WAJEZ2-4	Warsztaty kompetencji językowych II (j. angielski, j. niemiecki)	E	3	50	0	30	20											30	20
		RAZEM:		**6**	**100**	**0**	**60**	**40**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**30**	**20**	**0**	**30**	**20**

Moduły praktyk kierunkowych

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S2-00-PRAKTYKA1-2	Praktyka kierunkowa 1	ZAL	9	240	2	10	228				2	10	228						
2					0	0	0	0												
		RAZEM:		**9**	**240**	**2**	**10**	**228**	**0**	**0**	**0**	**2**	**10**	**228**	**0**	**0**	**0**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr											
						sem. 1			sem. 2			sem. 3			sem 4		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	246	106	126	14	106	126	14	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	550	166	354	30	0	72	0	86	106	0	30	70	20	50	106	10
3	Moduły przygotowania pracy dyplomowej	108	0	98	10	0	0	0	0	30	10	0	32	0	0	36	0
4	Moduły kształcenia językowego	100	0	60	40	0	0	0	0	0	0	0	30	20	0	30	20
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Razem bez modułu praktyk kierunkowych:	**1004**	**272**	**638**	**94**	**106**	**198**	**14**	**86**	**136**	**10**	**30**	**132**	**40**	**50**	**172**	**30**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
6	Moduły praktyk kierunkowych	240	2	10	228	0	0	0	2	10	228	0	0	0	0	0	0
	RAZEM z modułem praktyk kierunkowych:	**1244**				**318**			**472**			**202**			**252**		

Punkty ECTS

Lp.		Liczba punktów	Semestr			
			sem. 1	sem. 2	sem. 3	sem 4
1	Moduły kształcenia podstawowego	19	19	0	0	0
2	Moduły kształcenia kierunkowego	42	6	15	9	12
3	Moduły przygotowania pracy dyplomowej	13	0	4	4	5
4	Moduły kształcenia językowego	6	0	0	3	3
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0
6	Moduły praktyk kierunkowych	9	0	9	0	0
	RAZEM:	**89**	**25**	**28**	**16**	**20**
	Moduł kształcenia specjalnościowego:	*31*	*5*	*2*	*14*	*10*
	OGÓŁEM:	**120**	**30**	**30**	**30**	**30**
	Dopuszczalny deficyt punktowy po semetrze:		-5	-5	-5	-5

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Zarządzanie bezpieczeństwem sztucznej inteligencji*
Stopień kształcenia: studia drugiego stopnia **Czas trwania:** 4 semestry
Forma studiów: stacjonarne **Obowiązuje od roku akademickiego:** 2026/2027
Profil: praktyczny

Moduły kształcenia specjalnościowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S2-00-BEZDDANAI-2	Bezpieczeństwo danych, prywatność i bias w AI	O	3	36	0	36	0					36							
2	S2-00-NORPRWAI-2	Normy i uwarunkowania prawne AI	O	4	50	20	30	0				20	30							
3	S2-00-MODIMPAI-4	Modele implementacji sztucznej inteligencji	O	5	60	30	30	0										30	30	
4	S2-00-AISYBINFR-3	AI w systemach bezpieczeństwa, infrastrukturze krytycznej i IoT	O	5	60	30	30	0							30	30				
5	S2-00-AIGOVRISK-3	Nadzór nad AI i zarządzanie ryzykiem	O	2	30	0	30	0								30				
6	S2-00-AUTOAISEC-4	Automatyzacja i integracja AI w systemach bezpieczeństwa	O	2	30	0	30	0											30	
RAZEM:				**21**	**266**	**80**	**186**	**0**	**0**	**0**	**0**	**20**	**66**	**0**	**30**	**60**	**0**	**30**	**60**	**0**

Moduły praktyk specjalnościowych

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228							2	10	228			
2					0	0	0	0												
RAZEM:				**10**	**240**	**2**	**10**	**228**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**228**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr											
						sem. 1			sem. 2			sem. 3			sem 4		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	246	106	126	14	106	126	14	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	550	166	354	30	0	72	0	86	106	0	30	70	20	50	106	10
3	Moduły przygotowania pracy dyplomowej	108	0	98	10	0	0	0	0	30	10	0	32	0	0	36	0
4	Moduły kształcenia językowego	100	0	60	40	0	0	0	0	0	0	0	30	20	0	30	20
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	266	80	186	0	0	0	0	20	66	0	30	60	0	30	60	0
Ogółem bez praktyk		**1270**	**352**	**824**	**94**	**106**	**198**	**14**	**106**	**202**	**10**	**60**	**192**	**40**	**80**	**232**	**30**
Moduły praktyk		Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	240	2	10	228	0	0	0	2	10	228	0	0	0	0	0	0
Ogółem praktyki		**480**	**4**	**20**	**456**	**0**	**0**	**0**	**2**	**10**	**228**	**2**	**10**	**228**	**0**	**0**	**0**
OGÓŁEM:		**1750**				**318**			**558**			**532**			**342**		

Punkty ECTS

Lp.		Liczba punktów	Semestr			
			sem. 1	sem. 2	sem. 3	sem 4
1	Moduły kształcenia podstawowego	19	19	0	0	0
2	Moduły kształcenia kierunkowego	42	6	15	9	12
3	Moduły przygotowania pracy dyplomowej	13	0	4	4	5
4	Moduły kształcenia językowego	6	0	0	3	3
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	21	0	7	7	7
Ogółem bez praktyk		**101**	**25**	**26**	**23**	**27**
7	Moduły praktyk kierunkowych	9	0	9	0	0
8	Moduły praktyk specjalnościowych	10	0	0	10	0
Ogółem praktyki		**19**	**0**	**9**	**10**	**0**
OGÓŁEM:		**120**	**25**	**35**	**33**	**27**

liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**1200**
Liczba godzin zajęć e-learningowych i projektów	**94**
Liczba godzin praktyk w Instytucji	**456**
Łączna liczba godzin w programie	**1750**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Zarządzanie audytami i jakością*
Stopień kształcenia: studia drugiego stopnia **Czas trwania:** 4 semestry
Forma studiów: stacjonarne **Obowiązuje od roku akademickiego:** 2026/2027
Profil: praktyczny

Moduły kształcenia specjalnościowego

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S2-00-POLBEZGOD-2	Polityka bezpieczeństwa i zgodność w dobie regulacji cyfrowych	O	3	36	0	36	0					36							
2	S2-00-STRZARINC-2	Strategiczne zarządzanie incydentami – aspekty techniczne i psychologiczne	O	4	50	20	30	0				20	30							
3	S2-00-AUDYBEZIS-4	Audyt bezpieczeństwa informacji i systemów	O	5	60	30	30	0										30	30	
4	S2-00-CYBERGOV-3	Nadzór nad cyberbezpieczeństwem w organizacji	O	5	60	30	30	0							30	30				
5	S2-00-BUDWSTRB-3	Budowanie i wdrażanie strategii bezpieczeństwa organizacji	O	2	30	0	30	0								30				
6	S2-00-NOWNCOMP-4	Narzędzia wspierające zgodność z przepisami	O	2	30	0	30	0											30	
RAZEM:				**21**	**266**	**80**	**186**	**0**	**0**	**0**	**0**	**20**	**66**	**0**	**30**	**60**	**0**	**30**	**60**	**0**

Moduły praktyk specjalnościowych

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr											
									sem. 1			sem. 2			sem. 3			sem 4		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228							2	10	228			
2					0	0	0	0												
RAZEM:				**10**	**240**	**2**	**10**	**228**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**228**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr											
						sem. 1			sem. 2			sem. 3			sem 4		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	246	106	126	14	106	126	14	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	550	166	354	30	0	72	0	86	106	0	30	70	20	50	106	10
3	Moduły przygotowania pracy dyplomowej	108	0	98	10	0	0	0	0	30	10	0	32	0	0	36	0
4	Moduły kształcenia językowego	100	0	60	40	0	0	0	0	0	0	0	30	20	0	30	20
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	266	80	186	0	0	0	0	20	66	0	30	60	0	30	60	0
	Ogółem bez praktyk	**1270**	**352**	**824**	**94**	**106**	**198**	**14**	**106**	**202**	**10**	**60**	**192**	**40**	**80**	**232**	**30**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	240	2	10	228	0	0	0	2	10	228	0	0	0	0	0	0
8	Moduły praktyk specjalnościowych	240	2	10	228	0	0	0	0	0	0	2	10	228	0	0	0
	Ogółem praktyki	**480**	**4**	**20**	**456**	**0**	**0**	**0**	**2**	**10**	**228**	**2**	**10**	**228**	**0**	**0**	**0**
	OGÓŁEM:	**1750**				**318**			**558**			**532**			**342**		

Punkty ECTS

Lp.		Liczba punktów	Semestr			
			sem. 1	sem. 2	sem. 3	sem 4
1	Moduły kształcenia podstawowego	19	19	0	0	0
2	Moduły kształcenia kierunkowego	42	6	15	9	12
3	Moduły przygotowania pracy dyplomowej	13	0	4	4	5
4	Moduły kształcenia językowego	6	0	0	3	3
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	21	0	7	7	7
	Ogółem bez praktyk	**101**	**25**	**26**	**23**	**27**
7	Moduły praktyk kierunkowych	9	0	9	0	0
8	Moduły praktyk specjalnościowych	10	0	0	10	0
	Ogółem praktyki	**19**	**0**	**9**	**10**	**0**
	OGÓŁEM:	**120**	**25**	**35**	**33**	**27**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**1200**
Liczba godzin zajęć e-learningowych i projektów	**94**
Liczba godzin praktyk w Instytucji	**456**
Łączna liczba godzin w programie	**1750**

Macierz efektów uczenia się
Uczelnia: **Uniwersytet DSW Ideis**
Wydział: **Studiów Stosowanych we Wrocławiu**
Kierunek: **Zarządzanie cyberbezpieczeństwem**
Moduł kształcenia wybieralnego / w zakresie ***Zarządzanie audytami i jakością***
Stopień kształcenia: **Magister (II stopień)**
Profil: **Praktyczny**
Czas trwania **4 semestry**
Obowiązuje od roku akademickiego **2026/27**

OPIS KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ Po zakończeniu studiów absolwent osiąga następujące efekty uczenia się:	Symbol efektu uczenia się dla kierunku	Symbol charakterystyk	Stopień nasycenia efektu uczenia się	Moduły kształcenia podstawowego						Moduły kształcenia kierunkowego										Moduły kształcenia językowego		Moduły przygotowania pracy dyplomowej			Moduły praktyk kierunkowych		Moduły kształcenia wybieralnego (kształcenie w zakresie)					
				Współczesne wyzwania zarządzania	Współczesne zagrożenia bezpieczeństwa	Matematyka dyskretna	Psychologiczne aspekty cyberbezpieczeństwa	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	Szkolenie wstępne z zakresu BHP	Kontekst organizacji i zarządzanie interesariuszami	Kategorie cyberzagrożeń i podatności	Kryptografia i blockchain	Zarządzanie ryzykiem, kryzysowe i komunikacja	Zarządzanie zespołami różnorodnymi i rozwiązywanie konfliktów	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	Metodyki zarządzania projektami	Zarządzanie zmianą i transformacją cyfrową	Zarządzanie odpornością organizacji i ciągłością działania	Technologiczne trendy i wpływ na organizacje	Język obcy I (j.angielski, j.niemiecki)	Język obcy II (j.angielski, j.niemiecki)	Metodologia badań	Seminarium I	Seminarium II	Praktyka zawodowa kierunkowa I	Praktyka zawodowa kierunkowa II	Polityka bezpieczeństwa i zgodność w dobie regulacji cyfrowych	Strategiczne zarządzanie incydentami – aspekty techniczne i psychologiczne	Audyt bezpieczeństwa informacji i systemów	Nadzór nad cyberbezpieczeństwem w organizacji	Budowanie i wdrażanie strategii bezpieczeństwa organizacji	Narzędzia wspierające zgodność z przepisami
WIEDZA **absolwent zna i rozumie:**				**3**	**2**	**1**	**3**	**3**	**1**	**3**	**3**	**2**	**3**	**2**	**3**	**3**	**3**	**3**	**3**	**0**	**0**	**2**	**2**	**2**	**3**	**4**	**3**	**3**	**3**	**2**	**3**	**3**
Zna i rozumie w pogłębionym stopniu złożone koncepcje zarządzania organizacją i cyberbezpieczeństwem, uwzględniając ich współczesne ujęcia teoretyczne i praktyczne	ZCYB_II_W01	P7S_WG	**6**	x												x						x	x						x	x	
Zna i rozumie w pogłębionym stopniu modele współpracy interesariuszy oraz polityki bezpieczeństwa w skali międzynarodowej i krajowej	ZCYB_II_W02	P7S_WG	**5**					x		x															x		x			x		
Zna i rozumie w pogłębionym stopniu mechanizmy regulacyjne i prawne związane z ochroną danych, cyberbezpieczeństwem i standardami (NIS2, AI Act, DORA, RODO/GDPR)	ZCYB_II_W03	P7S_WG	**4**					x	x																		x					x
Zna i rozumie w pogłębionym stopniu typologie zagrożeń, ich struktury oraz wpływ na funkcjonowanie organizacji	ZCYB_II_W04	P7S_WG	**5**		x						x							x							x			x				
Zna i rozumie w pogłębionym stopniu architekturę systemów zarządzania bezpieczeństwem informacji oraz podstawy technologii kryptograficznych	ZCYB_II_W05	P7S_WG	**5**									x			x			x								x			x			
Zna i rozumie w pogłębionym stopniu metodyki zarządzania projektami, zmianą i ryzykiem w środowiskach cyfrowych	ZCYB_II_W06	P7S_WG	**6**	x									x			x	x						x						x		
Zna i rozumie stopniu wpływ psychologicznych i społecznych czynników na bezpieczeństwo organizacji i jej pracowników	ZCYB_II_W07	P7S_WK	**4**				x			x				x														x				
Zna i rozumie znaczenie oraz mechanizmy transformacji cyfrowej i innowacji technologicznych wpływających na bezpieczeństwo organizacji	ZCYB_II_W08	P7S_WK	**4**										x				x		x					x								
Zna i rozumie w pogłębionym stopniu modele i strategie zarządzania odpornością organizacji na zagrożenia cybernetyczne i kryzysy	ZCYB_II_W09	P7S_WG	**8**				x				x		x		x			x								x			x			
Zna i rozumie zastosowania sztucznej inteligencji w bezpieczeństwie, jej główne ryzyka oraz normy regulacyjne.	ZCYB_II_W10	P7S_WK	**4**					x				x							x							x						
Zna i rozumie zasady zarządzania zespołami różnorodnymi oraz rozwiązywania konfliktów w kontekście bezpieczeństwa	ZCYB_II_W11	P7S_WK	**4**	x						x				x		x																
Zna i rozumie w pogłębionym stopniu mechanizmy zapewniania zgodności i audytu bezpieczeństwa zgodne z aktualnymi wymogami prawa i standardami branżowymi	ZCYB_II_W12	P7S_WG	**5**																						x	x	x		x			x
Zna i rozumie znaczenie ochrony prywatności oraz zjawiska biasu w systemach sztucznej inteligencji	ZCYB_II_W13	P7S_WK	**3**												x		x												x			
Zna i rozumie w pogłębionym stopniu metody statystyczne i analityczne stosowane w ocenie ryzyka i efektywności strategii bezpieczeństwa	ZCYB_II_W14	P7S_WG	**5**			x					x								x			x										x
Zna i rozumie etyczne i społeczne konsekwencje zarządzania cyberbezpieczeństwem w dobie cyfryzacji i globalizacji	ZCYB_II_W15	P7S_WK	**3**		x		x																	x								

UMIEJĘTNOŚCI absolwent potrafi:				3	2	2	3	2	1	3	3	2	3	3	3	3	3	2	3	2	2	3	3	3	3	3	3	3	3	3	3	3
Potrafi samodzielnie tworzyć i wdrażać polityki bezpieczeństwa oraz strategie zarządzania ryzykiem cybernetycznym	ZCYB_II_U01	P7S_UW	**6**					x					x		x												x			x	x	
Potrafi prowadzić złożone analizy strategiczne w organizacjach o różnych profilach działalności	ZCYB_II_U02	P7S_UW	**7**	x						x				x		x	x											x			x	
Potrafi modelować oraz optymalizować procesy reagowania na incydenty oraz zarządzania ciągłością działania	ZCYB_II_U03	P7S_UW	**6**		x		x		x		x							x										x				
Potrafi realizować i nadzorować audyty bezpieczeństwa informacji zgodne ze standardami i wymaganiami prawnymi	ZCYB_II_U04	P7S_UW	**5**					x							x												x		x			x
Potrafi efektywnie komunikować się oraz współpracować z interesariuszami w środowisku wielosektorowym i międzykulturowym	ZCYB_II_U05	P7S_UK	**5**							x			x	x						x	x											
Potrafi wykorzystywać zaawansowane narzędzia IT, w tym rozwiązania oparte na sztucznej inteligencji, do monitoringu, analizy i automatyzacji procesów bezpieczeństw	ZCYB_II_U06	P7S_UW	**2**									x																				x
Potrafi identyfikować luki i zagrożenia w systemach bezpieczeństwa oraz formułować rekomendacje naprawcze	ZCYB_II_U07	P7S_UW	**4**		x						x	x																	x			
Potrafi zarządzać zmianami organizacyjnymi i technologicznymi, minimalizując opór i ryzyko	ZCYB_II_U08	P7S_UO	**4**				x						x				x														x	
Potrafi prowadzić negocjacje i mediacje w celu utrzymania zgodności i współpracy między zespołami	ZCYB_II_U09	P7S_UK	**5**	x			x							x		x												x				
Potrafi przygotowywać raporty strategiczne i analizy dla kierownictwa oraz organów regulacyjnych	ZCYB_II_U10	P7S_UK	**5**			x											x					x	x	x								
Potrafi integrować trendy innowacyjne oraz regulacje prawne w procesach podejmowania decyzji zarządczych	ZCYB_II_U11	P7S_UW	**5**	x												x		x					x							x		
Potrafi planować i prowadzić działania edukacyjne oraz szkoleniowe w obszarze cyberbezpieczeństwa	ZCYB_II_U12	P7S_UO	**5**							x								x				x		x	x							
Potrafi planowo rozwijać własne kompetencje oraz kompetencje zespołu zgodnie z potrzebami rynku i organizacji	ZCYB_II_U13	P7S_UU	**5**													x						x	x		x	x						
Potrafi krytycznie oceniać istniejące i proponować nowe rozwiązania zarządcze i techniczne w obszarze cyberbezpieczeństwa	ZCYB_II_U14	P7S_UW	**5**															x				x	x	x								x
Potrafi posługiwać się językiem obcym na poziomie umożliwiającym realizację obowiązków zawodowych w środowisku międzynarodowym, co odpowiada co najmniej poziomowi B2 według Europejskiego Systemu Opisu Kształcenia Językowego	ZCYB_II_U15	P7S_UK	**2**																	x	x											
Potrafi projektować systemy zarządzania efektywnością i ciągłym doskonaleniem bezpieczeństwa w organizacji	ZCYB_II_U16	P7S_UW	**3**												x												x			x		
Potrafi oceniać efektywność działań organizacji w obszarze ochrony przed zagrożeniami cybernetycznym	ZCYB_II_U17	P7S_UW	**4**			x					x											x							x			
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:				**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**2**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**2**	**1**	**0**	**2**	**1**	**2**	**3**	**1**	**2**	**2**	**1**
Jest gotów inicjować, planować i aktywnie realizować działania zespołowe oraz projekty organizacyjne i społeczne z zakresu zarządzania cyberbezpieczeństwem, wspierające rozwój kultury bezpieczeństwa informacji	ZCYB_II_K01	P7S_KO	**5**														x	x							x		x			x		
Jest gotów identyfikować potrzeby doskonalenia oraz proponować i wdrażać rozwiązania usprawniające system zarządzania cyberbezpieczeństwem, w tym procedury, procesy i narzędzia, z uwzględnieniem zasad zarządzania jakością	ZCYB_II_K02	P7S_KO	**10**		x			x			x	x			x				x							x	x	x		x		
Jest gotów brać odpowiedzialność za decyzje podejmowane w złożonych, niejednoznacznych sytuacjach związanych z cyberbezpieczeństwem oraz pełnić rolę lidera zespołu projektowego, operacyjnego lub kryzysowego	ZCYB_II_K03	P7S_KR	**10**	x									x	x		x	x	x					x		x			x		x		
Jest gotów efektywnie współpracować w zespołach interdyscyplinarnych, uwzględniając różne perspektywy interesariuszy, dbając o poszanowanie różnorodności oraz prowadzenie konstruktywnego dialogu, także w sytuacjach konfliktu lub presji decyzyjnej	ZCYB_II_K04	P7S_KO	**9**				x			x				x		x				x	x	x					x		x			
Jest gotów zapewniać jasną, rzetelną i przejrzystą komunikację w procesach zarządzania cyberbezpieczeństwem, w tym skuteczną koordynację zadań, raportowanie ryzyk i incydentów oraz budowanie zaufania w relacjach wewnętrznych i zewnętrznych	ZCYB_II_K05	P7S_KK	**9**	x		x	x		x	X			x									x					x					x

Macierz efektów uczenia się

Uczelnia:	**Uniwersytet DSW Ideis**
Wydział:	**Studiów Stosowanych we Wrocławiu**
Kierunek:	**Zarządzanie cyberbezpieczeństwem**
Moduł kształcenia wybieralnego / w zakresie	***Zarządzanie bezpieczeństwem Sztucznej Inteligencji***
Stopień kształcenia:	**Magister (II stopień)**
Profil:	**Praktyczny**
Czas trwania	**4 semestry**
Obowiązuje od roku akademickiego	**2026/27**

OPIS KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ Po zakończeniu studiów absolwent osiąga następujące efekty uczenia się:	**Symbol efektu uczenia się dla kierunku**	**Symbol charakterystyk**	**Stopień nasycenia efektu uczenia się**	Moduły kształcenia podstawowego						Moduły kształcenia kierunkowego										Moduły kształcenia językowego		Moduły przygotowania pracy dyplomowej			Moduły praktyk kierunkowych		Moduły kształcenia wybieralnego (kształcenie w zakresie)					
				Współczesne wyzwania zarządzania	Współczesne zagrożenia bezpieczeństwa	Matematyka dyskretna	Psychologiczne aspekty cyberbezpieczeństwa	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	Szkolenie wstępne z zakresu BHP	Kontekst organizacji i zarządzanie interesariuszami	Kategorie cyberzagrożeń i podatności	Kryptografia i blockchain	Zarządzanie ryzykiem, kryzysowe i komunikacja	Zarządzanie zespołami różnorodnymi i rozwiązywanie konfliktów	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	Metodyki zarządzania projektami	Zarządzanie zmianą i transformacją cyfrową	Zarządzanie odpornością organizacji i ciągłością działania	Technologiczne trendy i wpływ na organizację	Język obcy I (j.angielski, j.niemiecki)	Język obcy II (j.angielski, j.niemiecki)	Metodologia badań	Seminarium I	Seminarium II	Praktyka zawodowa kierunkowa I	Praktyka zawodowa kierunkowa II	Bezpieczeństwo danych, prywatność i bias w AI	Normy i uwarunkowania prawne AI	Modele implementacji sztucznej inteligencji	AI w systemach bezpieczeństwa, infrastrukturze krytycznej i IoT	Nadzór nad AI i zarządzanie ryzykiem	Automatyzacja i integracja AI w systemach bezpieczeństwa
WIEDZA absolwent zna i rozumie:				**3**	**2**	**1**	**3**	**3**	**1**	**3**	**3**	**2**	**3**	**2**	**3**	**3**	**3**	**3**	**3**	**0**	**0**	**2**	**2**	**2**	**3**	**4**	**3**	**3**	**3**	**2**	**2**	**3**
Zna i rozumie w pogłębionym stopniu złożone koncepcje zarządzania organizacją i cyberbezpieczeństwem, uwzględniając ich współczesne ujęcia teoretyczne i praktyczne	ZCYB_II_W01	P7S_WG	**4**	x												x						x	x									
Zna i rozumie w pogłębionym stopniu modele współpracy interesariuszy oraz polityki bezpieczeństwa w skali międzynarodowej i krajowej	ZCYB_II_W02	P7S_WG	**5**					x		x															x			x	x			
Zna i rozumie w pogłębionym stopniu mechanizmy regulacyjne i prawne związane z ochroną danych, cyberbezpieczeństwem i standardami (NIS2, AI Act, DORA, RODO/GDPR)	ZCYB_II_W03	P7S_WG	**4**					x	x																		x	x				
Zna i rozumie w pogłębionym stopniu typologie zagrożeń, ich struktury oraz wpływ na funkcjonowanie organizacji	ZCYB_II_W04	P7S_WG	**4**		x						x							x							x							
Zna i rozumie w pogłębionym stopniu architekturę systemów zarządzania bezpieczeństwem informacji oraz podstawy technologii kryptograficznych	ZCYB_II_W05	P7S_WG	**6**									x			x			x								x			x		x
Zna i rozumie w pogłębionym stopniu metodyki zarządzania projektami, zmianą i ryzykiem w środowiskach cyfrowych	ZCYB_II_W06	P7S_WG	**6**	x									x			x	x						x							x	
Zna i rozumie stopniu wpływ psychologicznych i społecznych czynników na bezpieczeństwo organizacji i jej pracowników	ZCYB_II_W07	P7S_WK	**3**				x			x				x																	
Zna i rozumie znaczenie oraz mechanizmy transformacji cyfrowej i innowacji technologicznych wpływających na bezpieczeństwo organizacji	ZCYB_II_W08	P7S_WK	**5**										x				x		x					x							x
Zna i rozumie w pogłębionym stopniu modele i strategie zarządzania odpornością organizacji na zagrożenia cybernetyczne i kryzysy	ZCYB_II_W09	P7S_WG	**6**				x				x		x		x			x								x					
Zna i rozumie zastosowania sztucznej inteligencji w bezpieczeństwie, jej główne ryzyka oraz normy regulacyjne.	ZCYB_II_W10	P7S_WK	**7**					x				x							x							x	x		x	x		
Zna i rozumie zasady zarządzania zespołami różnorodnymi oraz rozwiązywania konfliktów w kontekście bezpieczeństwa	ZCYB_II_W11	P7S_WK	**4**	x						x				x		x																
Zna i rozumie w pogłębionym stopniu mechanizmy zapewniania zgodności i audytu bezpieczeństwa zgodne z aktualnymi wymogami prawa i standardami branżowymi	ZCYB_II_W12	P7S_WG	**4**																						x	x		x			x	
Zna i rozumie znaczenie ochrony prywatności oraz zjawiska biasu w systemach sztucznej inteligencji	ZCYB_II_W13	P7S_WK	**4**												x		x										x					x
Zna i rozumie w pogłębionym stopniu metody statystyczne i analityczne stosowane w ocenie ryzyka i efektywności strategii bezpieczeństwa	ZCYB_II_W14	P7S_WG	**4**			x					x								x			x									
Zna i rozumie etyczne i społeczne konsekwencje zarządzania cyberbezpieczeństwem w dobie cyfryzacji i globalizacji	ZCYB_II_W15	P7S_WK	**4**		x		x																	x					x			

UMIEJĘTNOŚCI absolwent potrafi:				3	2	2	3	2	1	3	3	2	3	3	3	3	3	2	3	2	2	3	3	3	3	3	3	3	3	3	3	3
Potrafi samodzielnie tworzyć i wdrażać polityki bezpieczeństwa oraz strategie zarządzania ryzykiem cybernetycznym	ZCYB_II_U01	P7S_UW	5					x					x		x															x	x	
Potrafi prowadzić złożone analizy strategiczne w organizacjach o różnych profilach działalności	ZCYB_II_U02	P7S_UW	6	x						x				x		x	x													x		
Potrafi modelować oraz optymalizować procesy reagowania na incydenty oraz zarządzania ciągłością działania	ZCYB_II_U03	P7S_UW	6		x		x		x		x							x											x			
Potrafi realizować i nadzorować audyty bezpieczeństwa informacji zgodne ze standardami i wymaganiami prawnymi	ZCYB_II_U04	P7S_UW	3					x							x													x				
Potrafi efektywnie komunikować się oraz współpracować z interesariuszami w środowisku wielosektorowym i międzykulturowym	ZCYB_II_U05	P7S_UK	5							x			x	x						x	x											
Potrafi wykorzystywać zaawansowane narzędzia IT, w tym rozwiązania oparte na sztucznej inteligencji, do monitoringu, analizy i automatyzacji procesów bezpieczeństw	ZCYB_II_U06	P7S_UW	5									x															x	x	x			x
Potrafi identyfikować luki i zagrożenia w systemach bezpieczeństwa oraz formułować rekomendacje naprawcze	ZCYB_II_U07	P7S_UW	5		x						x	x																	x			x
Potrafi zarządzać zmianami organizacyjnymi i technologicznymi, minimalizując opór i ryzyko	ZCYB_II_U08	P7S_UO	4				x						x				x														x	
Potrafi prowadzić negocjacje i mediacje w celu utrzymania zgodności i współpracy między zespołami	ZCYB_II_U09	P7S_UK	4	x			x							x		x																
Potrafi przygotowywać raporty strategiczne i analizy dla kierownictwa oraz organów regulacyjnych	ZCYB_II_U10	P7S_UK	5			x												x				x	x	x								
Potrafi integrować trendy innowacyjne oraz regulacje prawne w procesach podejmowania decyzji zarządczych	ZCYB_II_U11	P7S_UW	5	x													x		x					x			x					
Potrafi planować i prowadzić działania edukacyjne oraz szkoleniowe w obszarze cyberbezpieczeństwa	ZCYB_II_U12	P7S_UO	5							x									x				x		x	x						
Potrafi planowo rozwijać własne kompetencje oraz kompetencje zespołu zgodnie z potrzebami rynku i organizacji	ZCYB_II_U13	P7S_UU	5													x						x	x		x	x						
Potrafi krytycznie oceniać istniejące i proponować nowe rozwiązania zarządcze i techniczne w obszarze cyberbezpieczeństwa	ZCYB_II_U14	P7S_UW	5																x					x	x	x		x				
Potrafi posługiwać się językiem obcym na poziomie umożliwiającym realizację obowiązków zawodowych w środowisku międzynarodowym, co odpowiada co najmniej poziomowi B2 według Europejskiego Systemu Opisu Kształcenia Językowego	ZCYB_II_U15	P7S_UK	2																	x	x											
Potrafi projektować systemy zarządzania efektywnością i ciągłym doskonaleniem bezpieczeństwa w organizacji	ZCYB_II_U16	P7S_UW	4												x															x	x		x
Potrafi oceniać efektywność działań organizacji w obszarze ochrony przed zagrożeniami cybernetycznym	ZCYB_II_U17	P7S_UW	4			x					x											x									x	
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:				2	1	1	2	1	1	2	1	1	2	2	1	2	2	2	1	1	1	2	1	0	2	1	2	1	2	2	1	1
Jest gotów inicjować, planować i aktywnie realizować działania zespołowe oraz projekty organizacyjne i społeczne z zakresu zarządzania cyberbezpieczeństwem, wspierające rozwój kultury bezpieczeństwa informacji	ZCYB_II_K01	P7S_KO	5														x	x							x				x		x	
Jest gotów identyfikować potrzeby doskonalenia oraz proponować i wdrażać rozwiązania usprawniające system zarządzania cyberbezpieczeństwem, w tym procedury, procesy i narzędzia, z uwzględnieniem zasad zarządzania jakością	ZCYB_II_K02	P7S_KO	10		x			x			x	x			x				x							x	x	x		x			
Jest gotów brać odpowiedzialność za decyzje podejmowane w złożonych, niejednoznacznych sytuacjach związanych z cyberbezpieczeństwem oraz pełnić rolę lidera zespołu projektowego, operacyjnego lub kryzysowego	ZCYB_II_K03	P7S_KR	9	x									x	x		x	x	x					x		x				x			
Jest gotów efektywnie współpracować w zespołach interdyscyplinarnych, uwzględniając różne perspektywy interesariuszy, dbając o poszanowanie różnorodności oraz prowadzenie konstruktywnego dialogu, także w sytuacjach konfliktu lub presji decyzyjnej	ZCYB_II_K04	P7S_KO	7				x			x				x		x				x	x	x										
Jest gotów zapewniać jasną, rzetelną i przejrzystą komunikację w procesach zarządzania cyberbezpieczeństwem, w tym skuteczną koordynację zadań, raportowanie ryzyk i incydentów oraz budowanie zaufania w relacjach wewnętrznych i zewnętrznych	ZCYB_II_K05	P7S_KK	10	x		x	x		x	X			x									x					x			x		x

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Zarządzanie bezpieczeństwem Sztucznej Inteligencji***

Stopień kształcenia: **II stopień**

Profil: **praktyczny**

Forma studiów: **niestacjonarne**

Czas trwania: **2 lata (4 semestry)**

Obowiązuje od roku akademickiego: **2026/27**

		SUMA W %						33,00%	3,17%	64,00%	74%	34%	44%	95%	5%	60%	40%
		SUMA PUNKTÓW ECTS	120					39,6	3,8	76,8	88,3	41,0	52,5	114,0	6,0	72,0	48,0
				Liczba godz.				Wskaźniki ECTS									
Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	ogół.	wyk.	ćw.	p/e	bezpośredni kontakt	Punkty ECTS za aktywność niewymagającą udziału nauczyciela akademickiego		praktyczne	wybieralne	z wykorzystaniem metod i technik kształcenia na odległość	zajęcia z dziedziny nauk społecznych	zajęcia z dziedziny nauk humanistycznych	dyscyplina wiodąca	dyscypliny uzupełniające
										e-learning	praca własna studenta						nauki o zarządzaniu i jakości	nauki o bezpieczeństwie
Moduły kształcenia podstawowego																			
1	N2-00-WSPWYZWZA-1	Współczesne wyzwania zarządzania	E	5	28	12	16	0	1,1	0,0	3,9	2,8	0,0	2,1	5,0		5,0	
2	N2-00-WSPZAGBEZ-1	Współczesne zagrożenia bezpieczeństwa	O	4	24	0	14	10	0,6	0,4	3,0	4,0	0,0	2,0	4,0			4,0
3	N2-00-MATDYSKRE-1	Matematyka dyskretna	O	4	20	0	20	0	0,8	0,0	3,2	4,0	0,0	2,0	4,0		4,0	
4	N2-00-ETPSYCHCYB-1	Etyka i psychologia cyberbezpieczeństwa	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5		3,0	2,0	1,0
5	N2-00-REGLPRAWC-1	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	O	3	18	18	0	0	0,7	0,0	2,3	0,0	0,0	3,0	3,0		2,0	1,0
6	N2-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,0	0,0			
Moduły kształcenia kierunkowego																			
1	N2-00-KONORGINT-1	Kontekst organizacji i zarządzanie interesariuszami	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5	3,0		3,0	
2	N2-00-KATCYBPOD-2	Kategorie cyberzagrożeń i podatności	O	3	16	16	0	0	0,6	0,0	2,4	0,0	0,0	3,0	3,0		0,0	3,0
3	N2-00-KRYPTBLCK-2	Kryptografia i blockchain	O	4	24	12	12	0	1,0	0,0	3,0	2,0	0,0	2,0	4,0			4,0
4	N2-00-ZARRYZYKR-2	Zarządzanie kryzysowe	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5	3,0		2,0	1,0
5	N2-00-KOMSPSYTZ-4	Komunikacja społeczna w sytuacjach zagrożeń cyfrowych	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5		3,0	3,0	

	N2-00-ZARZROZKO-4	Managing diverse teams and conflict resolution/ Management vielfältiger Teams und Konfliktlösung	O	4	24	12	12	0	1,0	0,0	3,0	2,0	4,0	2,0	4,0		4,0	
6	N2-00-ARCHITSZBI-3	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	E	5	36	12	14	10	1,0	0,4	3,6	3,4	0,0	1,7	5,0		2,0	3,0
7	N2-00-METZARPRJ-1	Metodyki zarządzania projektami	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5	3,0		3,0	
8	N2-00-ZARZMICTR-3	Zarządzanie zmianą i transformacją cyfrową	O	4	24	0	14	10	0,6	0,4	3,0	4,0	0,0	2,0	4,0		3,0	1,0
9	N2-00-ZARODPCIO-4	Zarządzanie odpornością organizacji i ciągłością działania	O	5	36	12	14	10	1,0	0,4	3,6	3,4	0,0	1,7	5,0		3,0	2,0
10	N2-00-TECHTRENOR-2	Technologiczne trendy i wpływ na organizacje	O	5	26	12	14	0	1,0	0,0	4,0	2,8	0,0	2,3	5,0		2,0	3,0
Moduły przygotowania pracy dyplomowej																		
1	N2-00-METTECBAD-2	Metody i techniki badań społecznych z elementami AI	O	4	24	0	14	10	0,6	0,4	3,0	4,0	0,0	2,0	4,0		3,0	1,0
2	N2-00-SEMMGR1-3	Seminarium magisterskie I	O	4	18	0	18	0	0,7	0,0	3,3	4,0	0,0	2,0	4,0		2,0	2,0
3	N2-00-SEMMGR2-4	Seminarium magisterskie II	O	5	20	0	20	0	0,8	0,0	4,2	5,0	0,0	2,5	5,0		3,0	2,0
Moduły kształcenia językowego																		
1	N2-00-WAJEZ1-3	Warsztaty kompetencji językowych I (j. angielski, j. niemiecki)	O	3	40	0	20	20	0,8	0,8	1,4		3,0	1,5	3,0		1,5	1,5
2	N2-00-WAJEZ2-4	Warsztaty kompetencji językowych II (j. angielski, j. niemiecki)	E	3	40	0	20	20	0,8	0,8	1,4		3,0	1,5	3,0		1,5	1,5
Moduły kształcenia specjalnościowego																		
1	N2-00-BEZDDANAI-2	Bezpieczeństwo danych, prywatność i bias w AI	O	3	16	0	16	0	0,6	0,0	2,4	3,0	3,0	1,5	3,0		2,0	1,0
2	N2-00-NORPRWAI-2	Normy i uwarunkowania prawne AI	O	4	20	20	0	0	0,8	0,0	3,2	0,0	4,0	4,0	4,0		2,0	2,0
3	N2-00-MODIMPAI-4	Modele implementacji sztucznej inteligencji	O	5	32	12	20	0	1,3	0,0	3,7	3,1	5,0	1,9	5,0		3,0	2,0
4	N2-00-AISYBINFR-3	AI w systemach bezpieczeństwa, infrastrukturze krytycznej i IoT	O	5	26	12	14	0	1,0	0,0	4,0	2,8	5,0	2,3	5,0		3,0	2,0
5	N2-00-AIGOVRISK-3	Nadzór nad AI i zarządzanie ryzykiem	O	2	14	0	14	0	0,6	0,0	1,4	2,0	2,0	1,0	2,0		2,0	
6	N2-00-AUTOAISEC-4	Automatyzacja i integracja AI w systemach bezpieczeństwa	O	2	14	0	14	0	0,6	0,0	1,4	2,0	2,0	1,0	2,0			2,0
Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	N2-00-PRAKTYKA1-2	Praktyka kierunkowa 1	ZAL	9	240	2	10	228	9,0	0,0	0,0	9,0		0,0	9,0		5,0	4,0
2	N2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228	9,6	0,0	0,4	10,0	10,0	0,0	10,0		6,0	4,0

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Zarządzanie audytami i jakością***

Stopień kształcenia: **II stopień**

Profil: **praktyczny**

Forma studiów: **niestacjonarne**

Czas trwania: **2 lata (4 semestry)**

Obowiązuje od roku akademickiego: **2026/27**

			SUMA W %					33,00%	3,17%	64,00%	74%	34%	44%	95%	5%	60%	40%
			SUMA PUNKTÓW ECTS	120				39,6	3,8	76,8	88,3	41,0	52,5	114,0	6,0	72,0	48,0
					Liczba godz.				Wskaźniki ECTS										
Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	ogół.	wyk.	ćw.	p/e	bezpośredni kontakt	Punkty ECTS za aktywność niewymagającą udziału nauczyciela akademickiego		praktyczne	wybieralne	z wykorzystaniem metod i technik kształcenia na odległość	zajęcia z dziedziny nauk społecznych	zajęcia z dziedziny nauk humanistycznych	dyscyplina wiodąca	dyscypliny uzupełniające
										e-learning	praca własna studenta						nauki o zarządzaniu i jakości	nauki o bezpieczeństwie
Moduły kształcenia podstawowego																			
1	N2-00-WSPWYZWZA-1	Współczesne wyzwania zarządzania	E	5	28	12	16	0	1,1	0,0	3,9	2,8	0,0	2,1	5,0		5,0	
2	N2-00-WSPZAGBEZ-1	Współczesne zagrożenia bezpieczeństwa	O	4	24	0	14	10	0,6	0,4	3,0	4,0	0,0	2,0	4,0			4,0
3	N2-00-MATDYSKRE-1	Matematyka dyskretna	O	4	20	0	20	0	0,8	0,0	3,2	4,0	0,0	2,0	4,0		4,0	
4	N2-00-ETPSYCHCYB-1	Etyka i psychologia cyberbezpieczeństwa	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5		3,0	2,0	1,0
5	N2-00-REGLPRAWC-1	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	O	3	18	18	0	0	0,7	0,0	2,3	0,0	0,0	3,0	3,0		2,0	1,0
6	N2-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,0	0,0			
Moduły kształcenia kierunkowego																			
1	N2-00-KONORGINT-1	Kontekst organizacji i zarządzanie interesariuszami	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5	3,0		3,0	
2	N2-00-KATCYBPOD-2	Kategorie cyberzagrożeń i podatności	O	3	16	16	0	0	0,6	0,0	2,4	0,0	0,0	3,0	3,0		0,0	3,0
3	N2-00-KRYPTBLCK-2	Kryptografia i blockchain	O	4	24	12	12	0	1,0	0,0	3,0	2,0	0,0	2,0	4,0			4,0
4	N2-00-ZARRYZYKR-2	Zarządzanie kryzysowe	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5	3,0		2,0	1,0
5	N2-00-KOMSPSYTZ-4	Komunikacja społeczna w sytuacjach zagrożeń cyfrowych	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5		3,0	3,0	

	N2-00-ZARZROZKO-4	Managing diverse teams and conflict resolution/ Management vielfältiger Teams und Konfliktlösung	O	4	24	12	12	0	1,0	0,0	3,0	2,0	4,0	2,0	4,0		4,0	
6	N2-00-ARCHITSZBI-3	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	E	5	36	12	14	10	1,0	0,4	3,6	3,4	0,0	1,7	5,0		2,0	3,0
7	N2-00-METZARPRJ-1	Metodyki zarządzania projektami	O	3	16	0	16	0	0,6	0,0	2,4	3,0	0,0	1,5	3,0		3,0	
8	N2-00-ZARZMICTR-3	Zarządzanie zmianą i transformacją cyfrową	O	4	24	0	14	10	0,6	0,4	3,0	4,0	0,0	2,0	4,0		3,0	1,0
9	N2-00-ZARODPCIO-4	Zarządzanie odpornością organizacji i ciągłością działania	O	5	36	12	14	10	1,0	0,4	3,6	3,4	0,0	1,7	5,0		3,0	2,0
10	N2-00-TECHTRENOR-2	Technologiczne trendy i wpływ na organizacje	O	5	26	12	14	0	1,0	0,0	4,0	2,8	0,0	2,3	5,0		2,0	3,0
Moduły przygotowania pracy dyplomowej																		
1	N2-00-METTECBAD-2	Metody i techniki badań społecznych z elementami AI	O	4	24	0	14	10	0,6	0,4	3,0	4,0	0,0	2,0	4,0		3,0	1,0
2	N2-00-SEMMGR1-3	Seminarium magisterskie I	O	4	18	0	18	0	0,7	0,0	3,3	4,0	0,0	2,0	4,0		2,0	2,0
3	N2-00-SEMMGR2-4	Seminarium magisterskie II	O	5	20	0	20	0	0,8	0,0	4,2	5,0	0,0	2,5	5,0		3,0	2,0
Moduły kształcenia językowego																		
1	N2-00-WAJEZ1-3	Warsztaty kompetencji językowych I (j. angielski, j. r	O	3	40	0	20	20	0,8	0,8	1,4		3,0	1,5	3,0		1,5	1,5
2	N2-00-WAJEZ2-4	Warsztaty kompetencji językowych II (j. angielski, j.	E	3	40	0	20	20	0,8	0,8	1,4		3,0	1,5	3,0		1,5	1,5
Moduły kształcenia specjalnościowego																		
1	N2-00-POLBEZGOD-2	Polityka bezpieczeństwa i zgodność w dobie regulacji cyfrowych	O	3	16	0	16	0	0,6	0,0	2,4	3,0	3,0	1,5	3,0		2,0	1,0
2	N2-00-STRZARINC-2	Strategiczne zarządzanie incydentami – aspekty	O	4	20	20	0	0	0,8	0,0	3,2	0,0	4,0	4,0	4,0		2,0	2,0
3	N2-00-AUDYBEZIS-4	Audyt bezpieczeństwa informacji i systemów	O	5	32	12	20	0	1,3	0,0	3,7	3,1	5,0	1,9	5,0		3,0	2,0
4	N2-00-CYBERGOV-3	Nadzór nad cyberbezpieczeństwem w organizacji	O	5	26	12	14	0	1,0	0,0	4,0	2,8	5,0	2,3	5,0		3,0	2,0
5	N2-00-BUDWSTRB-3	Budowanie i wdrażanie strategii bezpieczeństwa organizacji	O	2	14	0	14	0	0,6	0,0	1,4	2,0	2,0	1,0	2,0		2,0	
6	N2-00-NOWNCOMP-4	Narzędzia wspierające zgodność z przepisami	O	2	14	0	14	0	0,6	0,0	1,4	2,0	2,0	1,0	2,0			2,0
Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	N2-00-PRAKTYKA1-2	Praktyka kierunkowa 1	ZAL	9	240	2	10	228	9,0	0,0	0,0	9,0		0,0	9,0		5,0	4,0
2	N2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228	9,6	0,0	0,4	10,0	10,0	0,0	10,0		6,0	4,0

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Zarządzanie bezpieczeństwem Sztucznej Inteligencji***

Stopień kształcenia: **II stopień**

Profil: **praktyczny**

Forma studiów: **stacjonarne**

Czas trwania: **2 lata (4 semestry)**

Obowiązuje od roku akademickiego: **2026/27**

			SUMA W %						54,42%	3,17%	42,58%	73%	34%	41%	95%	5%	60%	40%
			SUMA PUNKTÓW ECTS	120					65,3	3,8	51,1	87,0	41,0	49,5	114,0	6,0	72,0	48,0
					Liczba godz.				Wskaźniki ECTS									
Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	ogół.	wyk.	ćw.	p/e	bezpośredni kontakt	Punkty ECTS za aktywność niewymagającą udziału nauczyciela akademickiego		praktyczne	wybieralne	z wykorzystaniem metod i technik kształcenia na odległość	zajęcia z dziedziny nauk społecznych	zajęcia z dziedziny nauk humanistycznych	dyscyplina wiodąca	dyscypliny uzupełniające
										e-learning	praca własna studenta						nauki o zarządzaniu i jakości	bezpieczeństwo, informatyka
Moduły kształcenia podstawowego																		
1	S2-00-WSPWYZWZA-1	Współczesne wyzwania zarządzania	E	5	70	30	40	0	2,8	0,0	2,2	2,9	0,0	2,1	5,0		5,0	
2	S2-00-WSPZAGBEZ-1	Współczesne zagrożenia bezpieczeństwa	O	4	50	20	20	10	1,6	0,4	2,0	2,4	0,0	1,6	4,0			4,0
3	S2-00-MATDYSKRE-1	Matematyka dyskretna	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	1,6	4,0		4,0	
4	S2-00-ETPSYCHCYB-1	Etyka i psychologia cyberbezpieczeństwa	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5		3,0	2,0	1,0
5	S2-00-REGLPRAWC-1	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	O	3	36	36	0	0	1,4	0,0	1,6	0,0	0,0	3,0	3,0		2,0	1,0
6	S2-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,0	0,0			
Moduły kształcenia kierunkowego																		
1	S2-00-KONORGINT-1	Kontekst organizacji i zarządzanie interesariuszami	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5	3,0		3,0	
2	S2-00-KATCYBPOD-2	Kategorie cyberzagrożeń i podatności	O	3	36	36	0	0	1,4	0,0	1,6	0,0	0,0	3,0	3,0		0,0	3,0
3	S2-00-KRYPTBLCK-2	Kryptografia i blockchain	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	1,6	4,0			4,0
4	S2-00-ZARRYZYKR-2	Zarządzanie kryzysowe	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5	3,0		2,0	1,0
5	S2-00-KOMSPSYTZ-4	Komunikacja społeczna w sytuacjach zagrożeń cyfrowych	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5		3,0	3,0	

	S2-00-ZARZROZKO-4	Managing diverse teams and conflict resolution/ Management vielfältiger Teams und Konfliktlösung	O	4	50	20	30	0	2,0	0,0	2,0	2,4	4,0	1,6	4,0		4,0	
6	S2-00-ARCHITSZBI-3	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	E	5	80	30	40	10	2,8	0,4	1,8	3,1	0,0	1,9	5,0		2,0	3,0
7	S2-00-METZARPRJ-1	Metodyki zarządzania projektami	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5	3,0		3,0	
8	S2-00-ZARZMICTR-3	Zarządzanie zmianą i transformacją cyfrową	O	4	40	0	30	10	1,2	0,4	2,4	4,0	0,0	2,0	4,0		3,0	1,0
9	S2-00-ZARODPCIO-4	Zarządzanie odpornością organizacji i ciągłością działania	O	5	80	30	40	10	2,8	0,4	1,8	3,1	0,0	1,9	5,0		3,0	2,0
10	S2-00-TECHTRENOR-2	Technologiczne trendy i wpływ na organizacje	O	5	70	30	40	0	2,8	0,0	2,2	2,9	0,0	2,1	5,0		2,0	3,0
Moduły przygotowania pracy dyplomowej																		
1	S2-00-METTECBAD-2	Metody i techniki badań społecznych z elementami AI	O	4	40	0	30	10	1,2	0,4	2,4	4,0	0,0	2,0	4,0		3,0	1,0
2	S2-00-SEMMGR1-3	Seminarium magisterskie I	O	4	32	0	32	0	1,3	0,0	2,7	4,0	0,0	2,0	4,0		2,0	2,0
3	S2-00-SEMMGR2-4	Seminarium magisterskie II	O	5	36	0	36	0	1,4	0,0	3,6	5,0	0,0	2,5	5,0		3,0	2,0
Moduły kształcenia językowego																		
1	S2-00-WAJEZ1-3	Warsztaty kompetencji językowych I (j. angielski, j. niemiecki)	O	3	50	0	30	20	1,2	0,8	1,0		3,0	1,5	3,0		1,5	1,5
2	S2-00-WAJEZ2-4	Warsztaty kompetencji językowych II (j. angielski, j. niemiecki)	E	3	50	0	30	20	1,2	0,8	1,0		3,0	1,5	3,0		1,5	1,5
Moduły kształcenia specjalnościowego																		
1	S2-00-BEZDDANAI-2	Bezpieczeństwo danych, prywatność i bias w AI	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	1,5	3,0		2,0	1,0
2	S2-00-NORPRWAI-2	Normy i uwarunkowania prawne AI	O	4	50	20	30	0	2,0	0,0	2,0	2,4	4,0	1,6	4,0		2,0	2,0
3	S2-00-MODIMPAI-4	Modele implementacji sztucznej inteligencji	O	5	60	30	30	0	2,4	0,0	2,6	2,5	5,0	2,5	5,0		3,0	2,0
4	S2-00-AISYBINFR-3	AI w systemach bezpieczeństwa, infrastrukturze krytycznej i IoT	O	5	60	30	30	0	2,4	0,0	2,6	2,5	5,0	2,5	5,0		3,0	2,0
5	S2-00-AIGOVRISK-3	Nadzór nad cyberbezpieczeństwem w organizacji	O	2	30	0	30	0	1,2	0,0	0,8	2,0	2,0	1,0	2,0		2,0	
6	S2-00-AUTOAISEC-4	Automatyzacja i integracja AI w systemach bezpieczeństwa	O	2	30	0	30	0	1,2	0,0	0,8	2,0	2,0	1,0	2,0			2,0
Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	S2-00-PRAKTYKA1-2	Praktyka kierunkowa 1	ZAL	9	240	2	10	228	9,0	0,0	0,0	9,0		0,0	9,0		5,0	4,0
2	S2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228	9,6	0,0	0,4	10,0	10,0	0,0	10,0		6,0	4,0

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Zarządzanie audytami i jakością***

Stopień kształcenia: **II stopień**

Profil: **praktyczny**

Forma studiów: **stacjonarne**

Czas trwania: **2 lata (4 semestry)**

Obowiązuje od roku akademickiego: **2026/27**

		SUMA W %							54,42%	3,17%	42,58%	73%	34%	41%	95%	5%	60%	40%
		SUMA PUNKTÓW ECTS		120					65,3	3,8	51,1	87,0	41,0	49,5	114,0	6,0	72,0	48,0
					Liczba godz.				Wskaźniki ECTS									
Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	ogół.	wyk.	ćw.	p/e	bezpośredni kontakt	Punkty ECTS za aktywność niewymagającą udziału nauczyciela akademickiego		praktyczne	wybieralne	z wykorzystaniem metod i technik kształcenia na odległość	zajęcia z dziedziny nauk społecznych	zajęcia z dziedziny nauk humanistycznych	dyscyplina wiodąca	dyscypliny uzupełniające
										e-learning	praca własna studenta						nauki o zarządzaniu i jakości	bezpieczeństwo, informatyka
Moduły kształcenia podstawowego																		
1	S2-00-WSPWYZWZA-1	Współczesne wyzwania zarządzania	E	5	70	30	40	0	2,8	0,0	2,2	2,9	0,0	2,1	5,0		5,0	
2	S2-00-WSPZAGBEZ-1	Współczesne zagrożenia bezpieczeństwa	O	4	50	20	20	10	1,6	0,4	2,0	2,4	0,0	1,6	4,0			4,0
3	S2-00-MATDYSKRE-1	Matematyka dyskretna	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	1,6	4,0		4,0	
4	S2-00-ETPSYCHCYB-1	Etyka i psychologia cyberbezpieczeństwa	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5		3,0	2,0	1,0
5	S2-00-REGLPRAWC-1	Regulacje prawne cyberbezpieczeństwa (NIS2, AI Act, DORA, RODO/GDPR)	O	3	36	36	0	0	1,4	0,0	1,6	0,0	0,0	3,0	3,0		2,0	1,0
6	S2-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,0	0,0			
Moduły kształcenia kierunkowego																		
1	S2-00-KONORGINT-1	Kontekst organizacji i zarządzanie interesariuszami	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5	3,0		3,0	
2	S2-00-KATCYBPOD-2	Kategorie cyberzagrożeń i podatności	O	3	36	36	0	0	1,4	0,0	1,6	0,0	0,0	3,0	3,0		0,0	3,0
3	S2-00-KRYPTBLCK-2	Kryptografia i blockchain	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	1,6	4,0			4,0
4	S2-00-ZARRYZYKR-2	Zarządzanie kryzysowe	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5	3,0		2,0	1,0
5	S2-00-KOMSPSYTZ-4	Komunikacja społeczna w sytuacjach zagrożeń cyfrowych	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5		3,0	3,0	

	S2-00-ZARZROZKO-4	Managing diverse teams and conflict resolution/ Management vielfältiger Teams und Konfliktlösung	O	4	50	20	30	0	2,0	0,0	2,0	2,4	4,0	1,6	4,0		4,0	
6	S2-00-ARCHITSZBI-3	Architektura Systemu Zarządzania Bezpieczeństwem Informacji	E	5	80	30	40	10	2,8	0,4	1,8	3,1	0,0	1,9	5,0		2,0	3,0
7	S2-00-METZARPRJ-1	Metodyki zarządzania projektami	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	1,5	3,0		3,0	
8	S2-00-ZARZMICTR-3	Zarządzanie zmianą i transformacją cyfrową	O	4	40	0	30	10	1,2	0,4	2,4	4,0	0,0	2,0	4,0		3,0	1,0
9	S2-00-ZARODPCIO-4	Zarządzanie odpornością organizacji i ciągłością działania	O	5	80	30	40	10	2,8	0,4	1,8	3,1	0,0	1,9	5,0		3,0	2,0
10	S2-00-TECHTRENOR-2	Technologiczne trendy i wpływ na organizacje	O	5	70	30	40	0	2,8	0,0	2,2	2,9	0,0	2,1	5,0		2,0	3,0
Moduły przygotowania pracy dyplomowej																		
1	S2-00-METTECBAD-2	Metody i techniki badań społecznych z elementami AI	O	4	40	0	30	10	1,2	0,4	2,4	4,0	0,0	2,0	4,0		3,0	1,0
2	S2-00-SEMMGR1-3	Seminarium magisterskie I	O	4	32	0	32	0	1,3	0,0	2,7	4,0	0,0	2,0	4,0		2,0	2,0
3	S2-00-SEMMGR2-4	Seminarium magisterskie II	O	5	36	0	36	0	1,4	0,0	3,6	5,0	0,0	2,5	5,0		3,0	2,0
Moduły kształcenia językowego																		
1	S2-00-WAJEZ1-3	Warsztaty kompetencji językowych I (j. angielski, j. niemiecki)	O	3	50	0	30	20	1,2	0,8	1,0		3,0	1,5	3,0		1,5	1,5
2	S2-00-WAJEZ2-4	Warsztaty kompetencji językowych II (j. angielski, j. niemiecki)	E	3	50	0	30	20	1,2	0,8	1,0		3,0	1,5	3,0		1,5	1,5
Moduły kształcenia specjalnościowego																		
1	S2-00-POLBEZGOD-2	Polityka bezpieczeństwa i zgodność w dobie regulacji cyfrowych	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	1,5	3,0		2,0	1,0
2	S2-00-STRZARINC-2	Strategiczne zarządzanie incydentami – aspekty	O	4	50	20	30	0	2,0	0,0	2,0	2,4	4,0	1,6	4,0		2,0	2,0
3	S2-00-AUDYBEZIS-4	Audyt bezpieczeństwa informacji i systemów	O	5	60	30	30	0	2,4	0,0	2,6	2,5	5,0	2,5	5,0		3,0	2,0
4	S2-00-CYBERGOV-3	Nadzór nad cyberbezpieczeństwem w organizacji	O	5	60	30	30	0	2,4	0,0	2,6	2,5	5,0	2,5	5,0		3,0	2,0
5	S2-00-BUDWSTRB-3	Budowanie i wdrażanie strategii bezpieczeństwa organizacji	O	2	30	0	30	0	1,2	0,0	0,8	2,0	2,0	1,0	2,0		2,0	
6	S2-00-NOWNCOMP-4	Narzędzia wspierające zgodność z przepisami	O	2	30	0	30	0	1,2	0,0	0,8	2,0	2,0	1,0	2,0			2,0
Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	S2-00-PRAKTYKA1-2	Praktyka kierunkowa 1	ZAL	9	240	2	10	228	9,0	0,0	0,0	9,0		0,0	9,0		5,0	4,0
2	S2-00-PRAKTSP1-3	Praktyka specjalnościowa I	ZAL	10	240	2	10	228	9,6	0,0	0,4	10,0	10,0	0,0	10,0		6,0	4,0