UNIWERSYTET DSW IDEIS
WYDZIAŁ STUDIÓW STOSOWANYCH WE WROCŁAWIU

PROGRAM STUDIÓW
NA KIERUNKU
Zarządzanie cyberbezpieczeństwem
STUDIA PIERWSZEGO 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 pierwszego stopnia	
Poziom kwalifikacji	6	
Profil studiów	praktyczny	
Forma studiów	stacjonarne / niestacjonarne	
Kod ISCED	0413	
Liczba semestrów konieczna do ukończenia studiów na ocenianym kierunku na danym poziomie	6	
Liczba punktów ECTS konieczna do ukończenia studiów na ocenianym kierunku na danym poziomie	180	
Łączna liczba godzin zajęć	stacjonarne 2764 godz.	niestacjonarne 2046 godz.
Wymiar praktyk zawodowych	960 godz.	
Język, w którym prowadzone są zajęcia	j. polski	
Tytuł zawodowy uzyskiwany przez absolwenta	Licencjat	
Uzyskiwane uprawnienia zawodowe	Brak	

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

O przyjęcie na studia mogą ubiegać się zarówno osoby posiadające obywatelstwo polskie, jak i obcokrajowcy, którzy uzyskali świadectwo dojrzałości lub jego odpowiednik w danym kraju uprawniający do ubiegania się o przyjęcie na studia wyższe. Warunkiem przyjęcia na studia jest zdobycie określonej liczby punktów wynikających z wyników egzaminu maturalnego oraz złożenie kompletu dokumentów, w tym zaświadczenia o stanie zdrowia i uiszczenie opłaty wpisowej.

O pierwszeństwie przyjęcia na studia decydować będzie ranking punktowy określony w zasadach rekrutacji. Do rankingu zaliczać się będą wyniki z kluczowych dla kierunku przedmiotów według następujących zasad (Konkurs, max 400 pkt):

- przedmiot obowiązkowy -do wyboru jeden: język polski, język obcy nowożytny, matematyka (1% na poziomie podstawowym = 1 pkt, 1% na poziomie rozszerzonym = 2 pkt);
- przedmiot dodatkowy -do wyboru jeden: informatyka, wiedza o społeczeństwie, matematyka; preferowane: informatyka, wiedza o społeczeństwie (×2). Wynik rekrutacyjny = punkty z przedmiotu obowiązkowego + punkty z przedmiotu dodatkowego (×2 jeżeli z listy preferowanych), max 400 pkt.

Kandydaci będą kwalifikowani według całkowitej liczby zdobytych punktów, rozpoczynając od osoby, która zdobyła najwyższą liczbę punktów, aż do wypełnienia limitu przyjęć na kierunek.

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	108,2	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	71,8	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	71,9 -97	71,9 -97
Łączna liczba punktów ECTS przyporządkowana zajęciom kształtującym umiejętności praktyczne	132,5 -137,7	132,5 -137,7
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	8	8
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	180	180
Łączna liczba punktów ECTS przyporządkowana zajęciom do wyboru	79,0	79,0
Łączna liczba punktów ECTS przyporządkowana praktykom zawodowym	38	38
W przypadku stacjonarnych studiów pierwszego stopnia i jednolitych studiów magisterskich liczba godzin zajęć z wychowania fizycznego	60	-
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	2764 / 234	2046 / 234

5. Sylwetka absolwenta

Absolwent studiów I stopnia na kierunku „Zarządzanie cyberbezpieczeństwem” posiada uporządkowaną wiedzę z zakresu zarządzania, podstaw ekonomii, prawa, technologii informacyjno-komunikacyjnych oraz bezpieczeństwa informacji, pozwalającą rozumieć funkcjonowanie organizacji w środowisku cyfrowym oraz istotę zagrożeń cybernetycznych. W obszarze umiejętności potrafi identyfikować i analizować zagrożenia, uczestniczyć w procesach zarządzania ryzykiem, monitorować zdarzenia bezpieczeństwa oraz wspierać procesy reagowania na incydenty, z uwzględnieniem współpracy z zespołami SOC i działami IT (W/U). W zakresie kompetencji społecznych jest przygotowany do pracy zespołowej, komunikacji z interesariuszami technicznymi i nietechnicznymi, prowadzenia podstawowych działań edukacyjnych z zakresu cyberhigieny oraz kształtowania odpowiedzialnych postaw wobec bezpieczeństwa cyfrowego i ochrony danych (K). Absolwent jest gotowy do podjęcia pracy na stanowiskach młodszego specjalisty ds. bezpieczeństwa informacji, członka zespołu SOC, asystenta ds. zarządzania ryzykiem lub koordynatora działań security awareness, a także do kontynuacji kształcenia na studiach II stopnia w obszarze zarządzania cyberbezpieczeństwem.

Specjalność: Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem

Absolwent specjalności „Biały wywiad w zarządzaniu cyberbezpieczeństwem” posiada wiedzę na temat źródeł otwartych (OSINT), metod pozyskiwania i analizy informacji, psychologicznych i społecznych uwarunkowań zachowań użytkowników oraz zagrożeń wynikających z czynnika ludzkiego. W zakresie umiejętności potrafi planować i realizować działania OSINT z poszanowaniem przepisów prawa i zasad etycznych, identyfikować luki informacyjne i podatności społeczno-techniczne, a także formułować wnioski i rekomendacje dla kadry zarządzającej (W/U). Rozwija kompetencje społeczne związane z odpowiedzialnym wykorzystywaniem informacji, komunikowaniem ryzyka związanego z użytkownikami oraz współpracą z zespołami bezpieczeństwa i audytu wewnętrznego (K).

Specjalność: Zarządzanie Zespołami Operacyjnymi IT

Absolwent specjalności „Zarządzanie zespołami operacyjnymi IT” dysponuje wiedzą dotyczącą ochrony infrastruktury IT, podstaw testów bezpieczeństwa, monitoringu bezpieczeństwa (w tym rozwiązań typu SIEM/SOAR) oraz organizacji pracy zespołów SOC. W obszarze umiejętności potrafi współorganizować procesy monitoringu, eskalacji i reagowania na incydenty, uczestniczyć w planowaniu i wdrażaniu środków ochrony oraz wspierać koordynację pracy zespołów technicznych (W/U). W zakresie kompetencji społecznych jest przygotowany do pełnienia ról młodszego koordynatora lub lidera zadaniowego, dbającego o komunikację w zespole, rzetelne raportowanie oraz przestrzeganie standardów etycznych i organizacyjnych w obszarze bezpieczeństwa (K).

Specjalność: Cyberhigiena i Edukacja Informacyjna

Absolwent specjalności „Cyberhigiena i edukacja informacyjna” posiada wiedzę z zakresu psychologii cyberzagrożeń, mechanizmów wpływu społecznego w środowisku cyfrowym, metod kształtowania świadomości użytkowników oraz projektowania programów edukacyjnych w obszarze bezpieczeństwa informacji. W obszarze umiejętności potrafi przygotowywać i prowadzić szkolenia, kampanie security awareness oraz działania profilaktyczne, dostosowując przekaz do różnych grup odbiorców, a także współpracować z kadrą zarządzającą przy wdrażaniu programów budowy kultury bezpieczeństwa (W/U). W zakresie kompetencji społecznych cechuje się wysoką wrażliwością etyczną, odpowiedzialnością za przekazywane treści oraz gotowością do pełnienia roli edukatora i wewnętrznego ambasadora bezpieczeństwa cyfrowego (K).

I. Koncepcja kształcenia

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

Przy formułowaniu koncepcji kształcenia na kierunku zarządzanie cyberbezpieczeństwem studia pierwszego 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 wprowadził do oferty edukacyjnej kierunek studiów zarządzanie cyberbezpieczeństwem, którego koncepcja kształcenia spełnia zarówno oczekiwania rynku, jak i samych studentów, odpowiadając na ich potrzeby oraz pasje.

Uniwersytet DSW Ideis w swoich założeniach strategicznych kładzie nacisk na wsparcie atrybutu praktyczności kształcenia, co na kierunku zarządzanie cyberbezpieczeństwem przejawiać się będzie w stosowanych metodach dydaktycznych, inwestycjach w specjalistyczne laboratoria oraz w zatrudnianiu wykwalifikowanych nauczycieli praktyków. Praktyczność kształcenia to również współpraca ze specjalistycznymi jednostkami działającymi w obszarze cyberbezpieczeństwa, takimi jak: CyberDefence24 - portal, którego misją jest edukacja i budowanie cyfrowej odporności Polski. Uczelnia dokłada wszelkich starań, aby tranzycja studentów z Uczelni na rynek pracy była jak najbardziej optymalna.

Koncepcja programu studiów była współtworzona i konsultowana z przedstawicielami środowiska cyberbezpieczeństwa, w tym z ekspertami z Defence Institute oraz CyberDefence24, a także specjalistami z branży IT i bezpieczeństwa informacji.

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, bezpieczeństwa informacji oraz technologii ICT, m.in. w takich miejscach jak centra operacji bezpieczeństwa (SOC), działy bezpieczeństwa IT, firmy konsultingowe z zakresu cyberbezpieczeństwa, organy administracji rządowej i samorządowej (CSIRT, ABW, NASK) oraz organizacje pozarządowe zajmujące się edukacją cyfrową.

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

Zarządzanie cyberbezpieczeństwem to kierunek studiów odpowiadający na jedno z najbardziej dynamicznie rosnących zapotrzebowań rynku pracy -zarówno w Polsce, jak i w całej Europie. Absolwenci tego kierunku wyposażeni są w konkretne, praktyczne kompetencje z pogranicza zarządzania, technologii i bezpieczeństwa informacji, które stanowią dziś fundament sprawnego funkcjonowania każdej organizacji, od mikroprzedsiębiorstwa po instytucję publiczną.

Cyberbezpieczeństwo należy do najszybciej rosnących branż na świecie. Wartość globalnego rynku cyberbezpieczeństwa wyniosła 219 mld USD w 2025 roku i według prognoz Fortune Business Insights wzrośnie do 699 mld USD do 2034 roku, przy skumulowanym rocznym wskaźniku wzrostu (CAGR) na poziomie 13,8%. Agencja Forrester prognozuje z kolei, że globalne wydatki na cyberbezpieczeństwo osiągną 302,5 mld USD do 2029 roku, rosnąc w tempie 14,4% CAGR. Wzrost ten jest napędzany przede wszystkim eskalacją cyberataków, przyspieszoną cyfryzacją gospodarki, ekspansją usług chmurowych oraz rosnącą presją regulacyjną.

Na poziomie europejskim rynek cyberbezpieczeństwa osiągnął wartość 56 mld USD w 2025 roku, a deficyt wykwalifikowanych specjalistów w UE sięgnął 299 000 osób w 2024 roku -co stanowi wzrost o 9% względem roku poprzedniego. Raport OECD wskazuje, że Europa jako całość mierzy się z luką wynoszącą ponad 300 000 specjalistów ds. cyberbezpieczeństwa, przy czym 76% organizacji ma trudności z pozyskaniem, a 71% z utrzymaniem odpowiedniej kadry. Według World Economic Forum „sieci komputerowe i cyberbezpieczeństwo" zajmują drugie miejsce wśród najszybciej rosnących kategorii kompetencji do 2030 roku, zaraz po AI i dużych zbiorach danych.

W Polsce sytuacja jest równie pilna. Wartość polskiego rynku cyberbezpieczeństwa osiągnęła 1,52 mld USD na koniec 2024 roku, a prognozy zakładają jego dalszy wzrost w tempie 5,85% rocznie do 2029 roku. Polska Izba Informatyki i Telekomunikacji (PIIT) szacuje niedobór specjalistów IT na ok. 50 000 osób, z czego nawet 10 000–15 000 stanowią specjaliści z zakresu cyberbezpieczeństwa. Aż 68% polskich przedsiębiorstw zgłasza brak wykwalifikowanej kadry w swoich zespołach odpowiedzialnych za bezpieczeństwo cyfrowe. Niedobór ten będzie systematycznie narastał -w 2024 roku liczba zgłoszeń potencjalnych incydentów obsługiwanych przez CERT Polska przekroczyła 600 000 (wzrost o 62% rok do roku), a liczba potwierdzonych incydentów bezpieczeństwa wzrosła o 29%, do ponad 100 000 przypadków dziennie. W 2025 roku liczba obsługiwanych incydentów przekroczyła 236 000, co oznacza podwojenie wartości rok do roku. Rada Ministrów przyjęła w marcu 2026 roku nową Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029, potwierdzając cyberbezpieczeństwo jako jeden z priorytetów polityki państwa.

Zapotrzebowanie na kadry w obszarze cyberbezpieczeństwa jest szczególnie silnie widoczne na Dolnym Śląsku, którego centrum stanowi Wrocław -trzecia co do wielkości lokalizacja sektora nowoczesnych usług

biznesowych w Polsce, zatrudniająca ok. 70 300 osób w centrach usług wspólnych i BPO (dane za I kw. 2025 r., ABSL, Sektor Usług Biznesowych w Polsce 2025). Blisko połowa centrów usług biznesowych działających w Polsce świadczy usługi z zakresu cyberbezpieczeństwa, co czyni ten sektor jednym z kluczowych pracodawców dla absolwentów kierunków bezpieczeństwa. We Wrocławiu swoje centra badawcze, operacyjne i GRC prowadzą m.in. EY GDS Poland, Accenture, Bank Millennium, Asseco Poland, Fidelity czy ArcelorMittal -wszystkie aktywnie rekrutujące specjalistów ds. bezpieczeństwa IT. Rynek pracy w Polsce dla branży security rośnie w tempie wyraźnie powyżej średniej IT: w 2024 roku liczba ofert pracy w kategorii „Security" wzrosła o 39% rok do roku, a w I połowie 2025 roku ogólna liczba ofert pracy IT zwiększyła się o 68% rok do roku, przy czym Security pozostaje jedną z najszybciej rosnących specjalizacji.

Nowym, silnym impulsem popytowym stały się regulacje europejskie. Dyrektywa NIS2, obowiązująca od 2024 roku, objęła nowe kategorie podmiotów (kluczowe i ważne) i nałożyła na nie formalne obowiązki w zakresie zarządzania ryzykiem, raportowania incydentów i bezpieczeństwa łańcucha dostaw. W Polsce implementacja NIS2 -w ramach nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC) -obejmie kilka tysięcy dodatkowych firm, z których każda będzie potrzebować co najmniej jednego przeszkolonego specjalisty. Rozporządzenie DORA, które zaczęło obowiązywać w sektorze finansowym w 2025 roku, wprowadza z kolei szczegółowe wymogi dotyczące odporności operacyjnej, testowania systemów i zarządzania dostawcami ICT. Szacuje się, że w Europie regulacje te przekładają się bezpośrednio na wzrost popytu na specjalistów z zakresu zgodności, ryzyka i zarządzania bezpieczeństwem -blisko 50% organizacji na rynkach europejskich przyznaje, że regulacje compliance wpływają na ich bieżące decyzje kadrowe.

Globalnie luka kadrowa w cyberbezpieczeństwie wynosi dziś 4,7–4,8 miliona specjalistów -szacunki Fortinetu (Cybersecurity Skills Gap Report 2025) wskazują wartość 4,7 mln, a dane ISC2 za 2024 rok -4,8 mln. Badanie ISC2 z 2025 roku pokazuje, że 33% organizacji nie jest w stanie zapewnić wystarczającej obsady zespołów bezpieczeństwa, a 88% doświadczyło co najmniej jednej poważnej konsekwencji wynikającej z niedoboru kompetencji w ciągu ostatnich 12 miesięcy. Jednocześnie raport Fortinetu wskazuje, że 86% firm odnotowało co najmniej jedno naruszenie bezpieczeństwa w 2024 roku, a 54% wskazuje brak umiejętności i szkoleń jako główną jego przyczynę.

Uniwersytet DSW, obserwując te trendy i wsłuchując się w potrzeby dolnośląskiego rynku pracy, opracował program studiów na kierunku „Zarządzanie cyberbezpieczeństwem" w taki sposób, by kształcić specjalistów zdolnych do podjęcia pracy od pierwszego dnia. Profil praktyczny, podział dyscyplinowy 60% (nauki o zarządzaniu i jakości) / 40% (nauki o bezpieczeństwie) oraz trzy specjalności -Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem, Zarządzanie Zespołami Operacyjnymi IT i Cyberhigiena i Edukacja Informacyjna - odpowiadają na konkretne role zawodowe poszukiwane na rynku: analityk SOC, specjalista OSINT, koordynator świadomości cyberbezpieczeństwa czy lider edukacji cyfrowej. Partnerstwo z CyberDefence24 -wiodącym polskim portalem informacyjnym i edukacyjnym w obszarze bezpieczeństwa cyfrowego -zapewnia studentom dostęp do aktualnej wiedzy praktycznej i kontaktów branżowych już w trakcie studiów.

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.:

Studia na kierunku zarządzanie cyberbezpieczeństwem pozwolą studentom:

- Wyposażenie studenta w uporządkowaną wiedzę z zakresu zarządzania, bezpieczeństwa informacji, niezbędną do rozumienia funkcjonowania organizacji w środowisku cyfrowym (W);
- Rozwinięcie umiejętności identyfikacji i analizy ryzyka, monitorowania zagrożeń oraz udziału w procesach reagowania na incydenty bezpieczeństwa, w tym we współpracy z zespołami SOC (U);
- Przygotowanie do współtworzenia i wdrażania podstawowych polityk, procedur oraz standardów bezpieczeństwa informacji i ochrony danych osobowych w organizacji (U);

- Kształtowanie kompetencji społecznych w obszarze komunikacji, pracy zespołowej, odpowiedzialnych postaw wobec bezpieczeństwa cyfrowego oraz zdolności prowadzenia działań edukacyjnych z zakresu cyberhigieny (K);
- Przygotowanie do kontynuowania kształcenia na studiach drugiego stopnia w obszarze zarządzania cyberbezpieczeństwem oraz kierunkach pokrewnych, poprzez ugruntowanie fundamentów teoretycznych i praktycznych (W/U/K).

Efekty uczenia się opracowane dla kierunku wpisują się w dziedzinę nauk społecznych. Mają one charakter praktyczny, co odpowiada celowi kształcenia na potrzeby rynku pracy.

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 sformułowanych w ramach celu operacyjnego: *Poprawa efektywności kształcenia* (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 województwa dolnośląskiego. W trakcie spotkań z interesariuszami zewnętrznymi kształtowały się propozycje modułów przedmiotów wybieralnych: Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem, Zarządzanie Zespołami Operacyjnymi IT oraz Cyberhigiena i Edukacja Informacyjna.

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 ds. cyberbezpieczeństwa, menedżerowie IT, audytorzy bezpieczeństwa, eksperci z zakresu prawa nowych technologii oraz dydaktycy o znacznym dorobku naukowym posiadający również doświadczenie w praktyce zawodowej.

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 znaczne 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 środowiska zagrożeń i technologicznego otoczenia cyfrowego. Cechuje się etyczną i społeczną odpowiedzialnością zawodową w obszarze bezpieczeństwa informacji. Docenia znaczenie całożyciowego uczenia się i jest przygotowany do kontynuowania edukacji na studiach podyplomowych, MBA oraz studiach drugiego stopnia w zakresie zarządzania cyberbezpieczeństwem.

3. Ogólne cele uczenia się

Studia I stopnia na kierunku „Zarządzanie cyberbezpieczeństwem" realizowane są w profilu praktycznym i przygotowują absolwentów do samodzielnego i efektywnego działania w roli specjalistów operacyjnych w obszarze bezpieczeństwa informacji. Program łączy wiedzę z zakresu zarządzania, prawa, technologii informacyjno-komunikacyjnych, psychologii oraz edukacji informacyjnej, kształtując zdolność rozumienia zarówno technicznych, jak i organizacyjnych i psychospołecznych uwarunkowań cyberbezpieczeństwa. Ogólne cele uczenia się na tym kierunku obejmują:

- **Wyposażenie studenta w uporządkowaną, interdyscyplinarną wiedzę o środowisku cyfrowym i jego zagrożeniach.** Absolwent powinien rozumieć funkcjonowanie organizacji w środowisku cyfrowym, znać podstawy ekonomii, prawa, technologii informacyjno-komunikacyjnych oraz bezpieczeństwa informacji w

stopniu umożliwiającym identyfikację i ocenę zagrożeń cybernetycznych. Wiedza ta stanowi fundament dla wszystkich dalszych kompetencji zawodowych i obejmuje zarówno znajomość regulacji krajowych i unijnych (m.in. RODO, KSC, NIS2), jak i rozumienie psychospołecznych uwarunkowań cyberbezpieczeństwa, w tym roli czynnika ludzkiego w incydentach i naruszeniach.

- **Rozwinięcie umiejętności identyfikacji, analizy i monitorowania ryzyka oraz reagowania na incydenty.** Absolwent powinien być zdolny do samodzielnego rozpoznawania zagrożeń, przeprowadzania podstawowej analizy ryzyka, uczestniczenia w procesach monitorowania zdarzeń bezpieczeństwa oraz wspierania procedur reagowania na incydenty — w tym we współpracy z zespołami centrum operacji bezpieczeństwa (SOC) i działami IT. Umiejętności te odpowiadają na konkretne, pilne zapotrzebowanie rynku pracy na analityków bezpieczeństwa zdolnych do operacyjnego działania od pierwszego dnia zatrudnienia.

- Przygotowanie do współtworzenia i wdrażania polityk, procedur i standardów bezpieczeństwa informacji. Absolwent powinien potrafić uczestniczyć w projektowaniu i wdrażaniu podstawowych polityk bezpieczeństwa informacji, procedur ochrony danych osobowych oraz standardów organizacyjnych w obszarze cyberbezpieczeństwa. Cel ten obejmuje umiejętność pracy z dokumentacją systemów zarządzania bezpieczeństwem, znajomość metodyki ISMS oraz zdolność dostosowywania rozwiązań do specyfiki organizacji, w której absolwent podejmie zatrudnienie.

- **Kształtowanie praktycznych kompetencji specjalnościowych — wywiadu w otwartych źródłach (OSINT), zarządzania operacjami IT lub edukacji informacyjnej.** Program zakłada pogłębienie kompetencji w jednej z trzech specjalności: Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem, Zarządzanie Zespołami Operacyjnymi IT lub Cyberhigiena i Edukacja Informacyjna. Każda z nich odpowiada na zidentyfikowane, konkretne role zawodowe poszukiwane na rynku, zapewniając absolwentowi wyraźną specjalizację przy jednoczesnym zachowaniu szerokiego profilu ogólnego. Realizacja zajęć praktycznych z udziałem partnerów branżowych — w tym CyberDefence24 — gwarantuje aktualność treści programowych i bezpośredni kontakt z realiami zawodowymi.

- Rozwijanie odpowiedzialnych postaw zawodowych, kompetencji komunikacyjnych i gotowości do uczenia się przez całe życie. Absolwent powinien być przygotowany do pracy zespołowej i komunikacji zarówno z interesariuszami technicznymi, jak i nietechnicznymi, prowadzenia podstawowych działań edukacyjnych z zakresu cyberhigieny oraz kształtowania kultury bezpieczeństwa w organizacji. Studia przygotowują jednocześnie do kontynuacji kształcenia na poziomie magisterskim, kładąc fundamenty pod dalszy rozwój w obszarze strategicznego zarządzania cyberbezpieczeństwem — zgodnie z ideą uczenia się przez całe życie (LLL) i wymogami szybko zmieniającego się środowiska cyfrowych zagrożeń.

Poprzez realizację tych celów, studenci kierunku Zarządzanie Cyberbezpieczeństwem są przygotowywani do efektywnego działania zarówno w sektorze publicznym, prywatnym, jak i non-profit, stając się wykwalifikowanymi specjalistami posiadającymi niezbędną wiedzę i umiejętności do odnoszenia sukcesów w dynamicznym środowisku cyberbezpieczeństwa.

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
I	studia pierwszego 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:	
6	poziom 6 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_I_	kierunkowe efekty uczenia się dla studiów pierwszego stopnia kierunku Zarządzanie Cyberbezpieczeństwem
W	kategoria wiedzy
U	kategoria umiejętności
K	kategoria kompetencji społecznych
P6S_WG	poziom 6 Polskiej Ramy Kwalifikacji kategoria wiedza: zna i rozumie/zakres i głębia
P6S_WK	poziom 6 Polskiej Ramy Kwalifikacji kategoria wiedza: zna i rozumie/kontekst
P6S_UW	poziom 6 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/wykorzystanie wiedzy
P6S_UK	poziom 6 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/komunikowanie się
P6S_UO	poziom 6 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/organizacja pracy
P6S_UU	poziom 6 Polskiej Ramy Kwalifikacji kategoria umiejętności: potrafi/uczenie się
P6S_KK	poziom 6 Polskiej Ramy Kwalifikacji kategoria kompetencje społeczne: jest gotów do/oceny
P6S_KO	poziom 6 Polskiej Ramy Kwalifikacji kategoria kompetencje społeczne: jest gotów do/odpowiedzialność
P6S_KR	poziom 6 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 pierwszego stopnia na kierunku ***zarządzanie cyberbezpieczeństwem***, profil praktyczny, absolwent osiąga następujące efekty uczenia się:	**Symbol charakterystyk**
	WIEDZA -absolwent:	
ZCYB_I_W01	W zaawansowanym stopniu zna i opisuje kluczowe koncepcje zarządzania i cyberbezpieczeństwa oraz ich powiązania z funkcjonowaniem organizacji	P6U_W P6S_WG
ZCYB_I_W02	W zaawansowanym stopniu zna funkcje zarządzania oraz rozumie ich zastosowanie w praktyce organizacji	P6U_W P6S_WG
ZCYB_I_W03	W zaawansowanym stopniu zna elementy architektury systemów ICT oraz narzędzia wspierające zapewnienie bezpieczeństwa organizacji	P6U_W P6S_WG

ZCYB_I_W04	W zaawansowanym stopniu zna i klasyfikuje rodzaje zagrożeń, podatności i incydentów w cyberprzestrzeni oraz ich wpływ na funkcjonowanie organizacji	P6U_W P6S_WG
ZCYB_I_W05	W zaawansowanym stopniu zna i rozumie istotę strategii zarządzania bezpieczeństwem informacji, w tym procesy analizy ryzyka, audytu bezpieczeństwa oraz zarządzania ciągłością działania	P6U_W P6S_WK
ZCYB_I_W06	W zaawansowanym stopniu zna modele organizacyjne oraz rozumie zasady funkcjonowania zespołów operacyjnych w kontekście bezpieczeństwa	P6U_W P6S_WK
ZCYB_I_W07	W zaawansowanym stopniu zna normy, standardy i przepisy prawne wpływające na procesy zarządzania bezpieczeństwem informacji	P6U_W P6S_WG
ZCYB_I_W08	W zaawansowanym stopniu zna psychologiczne i społeczne aspekty cyberzagrożeń	P6U_W P6S_WG
ZCYB_I_W09	W zaawansowanym stopniu zna metody i techniki zarządzania projektami i procesami w obszarze bezpieczeństwa informacji	P6U_W P6S_WG
ZCYB_I_W10	W zaawansowanym stopniu zna i rozumie znaczenie zarządzania wiedzą i budowania kultury bezpieczeństwa w organizacji	P6U_W P6S_WG
ZCYB_I_W11	W zaawansowanym stopniu zna techniki monitorowania i analizy zagrożeń (SIEM/SOAR, OSINT) oraz ich zastosowanie w praktyce organizacyjnej	P6U_W P6S_WK
ZCYB_I_W12	W zaawansowanym stopniu zna zasady ochrony informacji, danych osobowych, prywatności oraz etyki w środowisku cyfrowym	P6S_WK
ZCYB_I_W13	W zaawansowanym stopniu zna metody projektowania scenariuszy reakcji na incydenty oraz planów ciągłości działania organizacji	P6S_WK
ZCYB_I_W15	W zaawansowanym stopniu zna i rozumie znaczenie społecznej odpowiedzialności i konsekwencje działań związanych z cyberbezpieczeństwem	P6S_WK
UMIEJĘTNOŚCI -absolwent:		
ZCYB_I_U01	Umie analizować i oceniać problemy organizacyjne oraz zagrożenia cybernetyczne, proponując adekwatne rozwiązania zarządcze i techniczne	P6U_U P6S_UW
ZCYB_I_U02	Umie prowadzić skuteczną komunikację oraz koordynować działania w sytuacjach kryzysowych	P6U_U P6S_UK
ZCYB_I_U03	Umie wykorzystywać techniki OSINT i narzędzia analityczne w identyfikacji podatności i analizie ryzyka	P6S_UW
ZCYB_I_U04	Umie projektować i realizować działania rozwijające i wspierające kulturę bezpieczeństwa w organizacji	P6U_U P6S_UO
ZCYB_I_U05	Umie przeprowadzać audyty i testy bezpieczeństwa oraz opracowywać stosowną dokumentację zgodnie z obowiązującymi standardami	P6S_UW
ZCYB_I_U06	Umie stosować narzędzia do monitoringu oraz analizy cyberzagrożeń (SIEM, SOAR, OSINT) i oceniać efektywność zabezpieczeń	P6S_UW

ZCYB_I_U07	Umie opracowywać, wdrażać i aktualizować procedury reagowania na incydenty bezpieczeństwa informacji	P6S_UW
ZCYB_I_U08	Umie stosować strategie zarządzania zmianą i dostosowywac działania organizacyjne do dynamicznego otoczenia technologicznego	P6S_UW
ZCYB_I_U09	Umie planować, organizować i kontrolować zadania zespołów oraz zarządzać projektami w obszarze bezpieczeństwa informacji	P6U_U P6S_UO
ZCYB_I_U10	Umie planować i realizować działania zapewniające ciągłość działania oraz organizować reakcje awaryjne	P6S_UW
ZCYB_I_U11	Umie stosować przepisy prawne, normy branżowe i zasady etyki w praktyce zawodowej w zakresie zarządzania bezpieczeństwem	P6S_UW
ZCYB_I_U12	Umie efektywnie współpracować w zespołach interdyscyplinarnych oraz komunikować się z różnymi grupami interesariuszy	P6U_U P6S_UK
ZCYB_I_U13	Umie przygotowywać raporty i prezentacje opisujące stany i incydenty bezpieczeństwa, rekomendując działania zaradcze	P6S_UK
ZCYB_I_U15	Umie planować i wdrażać działania podnoszące świadomość i kulturę bezpieczeństwa w organizacji;	P6S_UO
ZCYB_I_U16	Umie posługiwać się językiem obcym (na poziomie B2 ESOKJ) w zakresie zarządzania i cyberbezpieczeństwa;	P6S_UK
ZCYB_I_U17	Umie krytycznie oceniać i aktualizować własną wiedzę oraz doskonalić kompetencje zawodowe w obszarze cyberbezpieczeństwa	P6S_UU
KOMPETENCJE SPOŁECZNE -absolwent:		
ZCYB_I_K01	Jest gotowy do współpracy w zespołach oraz skutecznej komunikacji z różnymi grupami interesariuszy w środowisku zawodowym	P6U_K P6S_KR
ZCYB_I_K02	Jest gotowy do uwzględniania konsekwencji społecznych, prawnych i etycznych działań w zakresie zarządzania cyberbezpieczeństwem	P6S_KO
ZCYB_I_K03	Jest gotowy do przestrzegania zasad etyki zawodowej i promowania kultury bezpieczeństwa informacji	P6S_KO
ZCYB_I_K04	Jest gotowy do krytycznej samooceny własnych kompetencji i planowania rozwoju zawodowego w obszarze zarządzania cyberbezpieczeństwem	P6U_K P6S_KK
ZCYB_I_K05	Jest gotowy do korzystania z wiedzy ekspertów i współpracy specjalistycznej w celu rozwiązywania problemów poznawczych i praktycznych	P6S_KK
ZCYB_I_K07	Jest gotowy do otwartego przyjmowania krytyki i dążenia do stałego rozwoju osobistego oraz zespołowego;	P6S_KR
ZCYB_I_K08	Jest gotowy do kształtowania proaktywnej postawy w dzieleniu się wiedzą i doświadczeniami	P6S_KO

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:		
P6U_W	w zaawansowanym stopniu -fakty, teorie, metody oraz złożone zależności między nimi różnorodne, złożone uwarunkowania prowadzonej działalności	ZCYB_I_W01 ZCYB_I_W02 ZCYB_I_W03 ZCYB_I_W04 ZCYB_I_W05 ZCYB_I_W06 ZCYB_I_W07 ZCYB_I_W08 ZCYB_I_W09 ZCYB_I_W10 ZCYB_I_W11 ZCYB_I_W12 ZCYB_I_W13 ZCYB_I_W14 ZCYB_I_W15
P6S_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_I_W01 ZCYB_I_W02 ZCYB_I_W03 ZCYB_I_W04 ZCYB_I_W05 ZCYB_I_W06 ZCYB_I_W07 ZCYB_I_W08 ZCYB_I_W09 ZCYB_I_W10 ZCYB_I_W11
P6S_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_I_W05 ZCYB_I_W06 ZCYB_I_W11 ZCYB_I_W12 ZCYB_I_W13 ZCYB_I_W14 ZCYB_I_W15
UMIEJĘTNOŚCI absolwent potrafi:		
P6U_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_I_U01 ZCYB_I_U02 ZCYB_I_U04 ZCYB_I_U09 ZCYB_I_U12 ZCYB_I_U14 ZCYB_I_U17

P6S_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_I_U01 ZCYB_I_U03 ZCYB_I_U05 ZCYB_I_U06 ZCYB_I_U07 ZCYB_I_U08 ZCYB_I_U09 ZCYB_I_U10 ZCYB_I_U11
P6S_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_I_U02 ZCYB_I_U12 ZCYB_I_U13 ZCYB_I_U16
P6S_UO	planować i organizować pracę indywidualną oraz w zespole współdziałać z innymi osobami w ramach prac zespołowych (także o charakterze interdyscyplinarnym)	ZCYB_I_U04 ZCYB_I_U09 ZCYB_I_U14 ZCYB_I_U15
P6S_UU	samodzielnie planować i realizować własne uczenie się przez całe życie	ZCYB_I_U17
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:		
P6U_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_I_K01 ZCYB_I_K02 ZCYB_I_K03 ZCYB_I_K04 ZCYB_I_K05 ZCYB_I_K06 ZCYB_I_K07 ZCYB_I_K08
P6S_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_I_K04 ZCYB_I_K05
P6S_KO	wypełniania zobowiązań społecznych, współorganizowania działalności na rzecz środowiska społecznego inicjowania działania na rzecz interesu publicznego myślenia i działania w sposób przedsiębiorczy	ZCYB_I_K02 ZCYB_I_K03 ZCYB_I_K08
P6S_KR	odpowiedzialnego pełnienia ról zawodowych, w tym: – przestrzegania zasad etyki zawodowej i wymagania tego od innych, – dbałości o dorobek i tradycje zawodu	ZCYB_I_K01 ZCYB_I_K06 ZCYB_I_K07

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	452	180	268	4	252	80	168	4
2	Moduły kształcenia kierunkowego	648	210	398	40	394	102	252	40
3	Moduły przygotowania pracy dyplomowej	90	0	90	0	54	0	54	0
4	Moduły kształcenia językowego	252	0	72	180	228	0	48	180
5	Moduły kształcenia w zakresie kultury fizycznej	60	0	60	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	284	40	234	10	158	26	122	10
7	Moduły praktyk kierunkowych	800	6	30	764	800	6	30	764
8	Moduły praktyk specjalnościowych	160	2	10	148	160	2	10	148

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 czy prawa nowych technologii. 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 w obszarze cyberbezpieczeństwa.

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
Kompetencje przyszłości II i III	4	4
Moduły kształcenia wybieralnego / specjalnościowego:	23	23
Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem		
Zarządzanie Zespołami Operacyjnymi IT		
Cyberhigiena i Edukacja Informacyjna		
Moduły praktyk kierunkowych	19	19
Seminarium I i II	10	10
Łącznie	**56**	**56**

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

Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem

Celem modułu jest wykształcenie specjalistów z zakresu białego wywiadu (OSINT) w kontekście zarządzania cyberbezpieczeństwem. Absolwenci specjalności będą przygotowani do prowadzenia działań wywiadowczych opartych na otwartych źródłach informacji, analizy podatności i ryzyk wynikających z czynnika ludzkiego oraz wspierania kadry zarządzającej w podejmowaniu decyzji.

Absolwent w czasie studiów zdobędzie wiedzę i umiejętności w zakresie:

- planowania i realizacji działań OSINT z poszanowaniem prawa i zasad etycznych;
- identyfikacji luk informacyjnych i podatności społeczno-technicznych;
- analizy psychologicznych i społecznych uwarunkowań zachowań użytkowników;
- formułowania wniosków i rekomendacji dla kadry zarządzającej;
- odpowiedzialnego wykorzystywania informacji i komunikowania ryzyka.

Moduł kształcenia wybieralnego ma przygotować studentów do podjęcia pracy na takich stanowiskach, jak:

- analityk OSINT,

- specjalista ds. threat intelligence,
- analityk ryzyka i podatności,
- koordynator security awareness,
- konsultant ds. bezpieczeństwa informacji.

Zarządzanie Zespołami Operacyjnymi IT

Celem modułu jest przygotowanie absolwentów do pełnienia ról koordynatorów i liderów zespołów operacyjnych w środowisku bezpieczeństwa IT. Studenci zdobedą kompetencje niezbędne do zarządzania procesami monitoringu, eskalacji i reagowania na incydenty.

Absolwent w czasie studiów zdobedzie wiedzę i umiejętności z zakresu:

- ochrony infrastruktury IT i podstaw testów bezpieczeństwa;
- monitoringu bezpieczeństwa z wykorzystaniem rozwiązań SIEM/SOAR;
- organizacji pracy zespołów SOC i koordynacji reagowania na incydenty;
- planowania i wdrażania środków ochrony technicznej;
- raportowania i komunikacji w sytuacjach kryzysowych.

Moduł kształcenia wybieralnego ma przygotować studentów do podjęcia pracy na takich stanowiskach, jak:

- analityk SOC (Security Operations Center),
- koordynator reagowania na incydenty,
- specjalista ds. monitoringu bezpieczeństwa,
- administrator bezpieczeństwa IT,
- junior manager ds. bezpieczeństwa informacji.

Cyberhigiena i Edukacja Informacyjna

Celem modułu jest przygotowanie absolwentów do pełnienia roli edukatora i koordynatora programów budowania świadomości bezpieczeństwa w organizacji.

Absolwent w czasie studiów zdobędzie wiedzę i umiejętności z zakresu:

- psychologii cyberzagrożeń i mechanizmów wpływu społecznego w środowisku cyfrowym;
- projektowania programów edukacyjnych w obszarze bezpieczeństwa informacji;
- przygotowywania i prowadzenia szkoleń i kampanii security awareness;
- kształtowania kultury bezpieczeństwa informacji w organizacji;
- etycznych aspektów przekazywania treści w środowisku cyfrowym.

Moduł kształcenia wybieralnego ma przygotować studentów do podjęcia pracy na takich stanowiskach, jak:

- specjalista ds. security awareness,
- edukator cyfrowy,
- trener z zakresu cyberbezpieczeństwa,
- koordynator programów budowania kultury bezpieczeństwa,
- ambasador bezpieczeństwa cyfrowego w organizacji.

4. Wymiar, zasady i formy odbywania praktyk zawodowych

W programie kształcenia dla kierunku zarządzanie cyberbezpieczeństwem o profilu praktycznym na studiach pierwszego stopnia przewidziano 960 godzin praktyk zawodowych (38 punktów ECTS), realizowanych w następującym wymiarze:

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

- centra operacji bezpieczeństwa (SOC) w firmach IT i instytucjach finansowych;
- działy bezpieczeństwa informacji i IT w przedsiębiorstwach;
- firmy konsultingowe z zakresu cyberbezpieczeństwa;
- organy administracji rządowej i samorządowej (CSIRT, ABW, NASK);
- instytucje zajmujące się audytem bezpieczeństwa;
- redakcje i portale specjalizujące się w cyberbezpieczeństwie (np. CyberDefence24);
- organizacje pozarządowe zajmujące się edukacją cyfrową.

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	Wprowadzenie do cyberbezpieczeństwa; Podstawy zarządzania; Podstawy ekonomii; Psychologia cyberbezpieczeństwa; Logika i krytyczne myślenie; Etyka i prywatność danych; Aspekty prawne i regulacje w cyberbezpieczeństwie; Technologie informatyczne; Kompetencje przyszłości I; Kompetencje przyszłości II; Kompetencje przyszłości III; Szkolenie wstępne z zakresu BHP
Moduły kształcenia kierunkowego	Systemy ICT w cyberbezpieczeństwie; Cyfrowe zarządzanie projektami (Gantt, Asana, Kanban); Zarządzanie ryzykiem w cyberprzestrzeni; Organizacja i zarządzanie; Cyberbezpieczeństwo operacyjne (wprowadzenie do narzędzi SIEM i SOAR, SOC); Warsztat pracy z grupą; Modelowanie cyberzagrożeń; Biały wywiad (OSINT) i analiza informacji; Testowanie i audyty cyberbezpieczeństwa; Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001); Analiza i zarządzanie podatnościami; Kultura bezpieczeństwa organizacji; Praktyki zarządzania incydentami; Podstawy Threat Intelligence; Socjologia dezinformacji i wojen informacyjnych; Role i uprawnienia w bezpieczeństwie informacji
Moduły kształcenia językowego	Język obcy I–III (język angielski, język niemiecki)

Moduły przygotowania pracy dyplomowej	Metodologia badań z elementami statystyki; Seminarium I; Seminarium II
Moduły kształcenia w zakresie kultury fizycznej	Wychowanie fizyczne I; Wychowanie fizyczne II
Moduły praktyk kierunkowych	Praktyka zawodowa ogólna I; Praktyka zawodowa ogólna II; Praktyka zawodowa kierunkowa I (wybieralna) -realizowane w instytucji zgodnie z regulaminem i programem praktyk na kierunku
Moduły kształcenia wybieralnego (kształcenie w zakresie) **Biały Wywiad w Zarządzaniu Cyberbezpieczeństwem**	Psychologia śledcza i profilowanie w cyberprzestrzeni; Psychologia poznawcza w wywiadzie i analizie danych; Zarządzanie stresem i efektywność pracy; Źródła danych dla białego wywiadu; OSINT i analiza behawioralna; Narzędzia i AI w służbie białego wywiadu; Analiza informacji i raportowanie; Design Thinking w cyberbezpieczeństwie;
Moduły kształcenia wybieralnego (kształcenie w zakresie) **Zarządzanie Zespołami Operacyjnymi IT**	Bezpieczeństwo fizyczne, środowiskowe i infrastruktury; Audyt incydentów i odporności; Testy penetracyjne i metody ofensywne; Współpraca SOC i zespołów ds. ryzyka; Narzędzia monitoringu i automatyzacji (SIEM i SOAR); Analiza strat i utrzymanie ciągłości operacyjnej; Tworzenie scenariuszy reakcji na incydenty; Zarządzanie stresem w trakcie ataku;
Moduły kształcenia wybieralnego (kształcenie w zakresie) **Cyberhigiena i Edukacja Informacyjna**	Cyberbezpieczeństwo wybranych grup społecznych -modele zarządzania ryzykiem; Strategie zarządzania ryzykiem ludzkim w organizacjach; Bezpieczeństwo organizacji wobec uzależnień technologicznych; Technologie wspierające edukację i monitorowanie efektywności; Projektowanie i zarządzanie narzędziami edukacyjnymi; Projektowanie interaktywnych szkoleń i e-learningu -aspekty wdrożeniowe; Wspieranie zdrowia psychicznego pracowników w środowisku cyfrowym; Metody badania efektywności programów edukacyjnych bezpieczeństwa;

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 pierwszego stopnia
Forma studiów: niestacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	32	14	18	0	14	18																
2	N1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	32	14	18	0	14	18																
3	N1-00-PODSTEKON-2	Podstawy ekonomii	O	4	28	12	16	0				12	16													
4	N1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	32	14	18	0				14	18													
5	N1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	32	14	18	0	14	18																
6	N1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	14	0	14	0					14													
7	N1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	28	12	16	0				12	16													
8	N1-00-TECHNINFO-1	Technologie informatyczne	O	3	14	0	14	0		14																
9	N1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	12	0	12	0		12																
10	N1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	12	0	12	0					12													
11	N1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	12	0	12	0								12										
12	N1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4			4															
		RAZEM:		**40**	**252**	**80**	**168**	**4**	**42**	**80**	**4**	**38**	**76**	**0**	**0**	**12**	**0**	**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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	32	14	18	0	14	18																
2	N1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	28	0	18	10					18	10												
3	N1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	20	0	20	0																	20	
4	N1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	28	12	16	0				12	16													
5	N1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	28	12	16	0				12	16													
6	N1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	14	0	14	0																	14	
7	N1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	30	0	20	10														20	10			
8	N1-00-OSINTANAL-1	Biały wywiad (OSINT) i analiza informacji	E	5	32	14	18	0	14	18																
9	N1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	34	12	12	10																12	12	10
10	N1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	28	12	16	0										12	16							
11	N1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	20	0	20	0											20							
12	N1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	20	0	20	0														20				
13	N1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	28	12	16	0																12	16	
14	N1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	14	14	0	0							14											
15	N1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	24	0	14	10											14	10						
16	N1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	14	0	14	0														14				
		RAZEM:		**55**	**394**	**102**	**252**	**40**	**28**	**36**	**0**	**24**	**50**	**10**	**14**	**0**	**0**	**12**	**50**	**10**	**0**	**54**	**10**	**24**	**62**	**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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-PROSEM-4	Metodologia badań	O	2	12	0	12	0											12							
2	N1-00-SEMDYP1-5	Seminarium I	O	3	18	0	18	0														18				
3	N1-00-SEMDYP2-6	Seminarium II	O	7	24	0	24	0																	24	
		RAZEM:		**12**	**54**	**0**	**54**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**12**	**0**	**0**	**18**	**0**	**0**	**24**	**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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	76	0	16	60								16	60									
2	N1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	76	0	16	60											16	60						
3	N1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	76	0	16	60														16	60			
		RAZEM:		**12**	**228**	**0**	**48**	**180**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**16**	**60**	**0**	**16**	**60**	**0**	**16**	**60**	**0**	**0**	**0**

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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308							2	10	308									
2	N1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148										2	10	148						
3	N1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I (wybieralna)	ZAL	13	320	2	10	308													2	10	308			
4					0	0	0	0																		
		RAZEM:		**32**	**800**	**6**	**30**	**764**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																				
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6					
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	252	80	168	4	42	80	4	38	76	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	394	102	252	40	28	36	0	24	50	10	14	0	0	12	50	10	0	54	10	24	62	10			
3	Moduły przygotowania pracy dyplomowej	54	0	54	0	0	0	0	0	0	0	0	0	0	0	12	0	0	18	0	0	24	0			
4	Moduły kształcenia językowego	228	0	48	180	0	0	0	0	0	0	0	16	60	0	16	60	0	16	60	0	0	0			
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Razem bez modułu praktyk kierunkowych:	**928**	**182**	**522**	**224**	**70**	**116**	**4**	**62**	**126**	**10**	**14**	**28**	**60**	**12**	**78**	**70**	**0**	**88**	**70**	**24**	**86**	**10**			
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.			
6	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0			
	RAZEM z modułem praktyk kierunkowych:	**1728**				**190**			**198**			**422**			**320**			**478**			**120**					

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
	RAZEM:	**151**	**30**	**30**	**21**	**22**	**28**	**20**
	Moduł kształcenia specjalnościowego:	*29*	*0*	*0*	*9*	*8*	*2*	*10*
	OGÓŁEM:	**180**	**30**	**30**	**30**	**30**	**30**	**30**
	Dopuszczalny deficyt punktowy po semetrze:		-5	-5	-5	-5	-5	-5

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Biały wywiad w zarządzaniu cyberbezpieczeństwem*
Stopień kształcenia: studia pierwszego stopnia
Forma studiów: niestacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-PSYCHSLED-3	Psychologia śledcza i profilowanie w cyberprzestrzeni	O	3	18	0	18	0								18										
2	N1-00-PSYCHPOZN-4	Psychologia poznawcza w wywiadzie i analizie danych	O	3	18	0	18	0											18							
3	N1-00-PSYCHPOZAN-3	Zarządzanie stresem i efektywność pracy	O	3	18	0	18	0								18										
4	N1-00-ZRODANOS-3	Źródła danych dla białego wywiadu	O	2	14	14	0	0							14											
5	N1-00-OSINTBEH-4	OSINT i analiza behawioralna	O	3	20	0	20	0											20							
6	N1-00-NARZAISLU-4	Narzędzia i AI w służbie białego wywiadu	O	3	20	0	20	0											20							
7	N1-00-ANALINFOR-5	Analiza informacji i raportowanie	O	3	24	12	12	0														12	12			
8	N1-00-DSGTHCYB-6	Design Thinking w cyberbezpieczenieństwie	O	3	26	0	16	10																	16	10
		RAZEM:		**23**	**158**	**26**	**122**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**14**	**36**	**0**	**0**	**58**	**0**	**12**	**12**	**0**	**0**	**16**	**10**

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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148																2	10	148
2					0	0	0	0																		
3					0	0	0	0																		
4					0	0	0	0																		
		RAZEM:		**6**	**160**	**2**	**10**	**148**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**148**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																			
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6				
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	252	80	168	4	42	80	4	38	76	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	394	102	252	40	28	36	0	24	50	10	14	0	0	12	50	10	0	54	10	24	62	10
3	Moduły przygotowania pracy dyplomowej	54	0	54	0	0	0	0	0	0	0	0	0	0	0	12	0	0	18	0	0	24	0
4	Moduły kształcenia językowego	228	0	48	180	0	0	0	0	0	0	0	16	60	0	16	60	0	16	60	0	0	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	158	26	122	10	0	0	0	0	0	0	14	36	0	0	58	0	12	12	0	0	16	10
	Ogółem bez praktyk	**1086**	**208**	**644**	**234**	**70**	**116**	**4**	**62**	**126**	**10**	**28**	**64**	**60**	**12**	**136**	**70**	**12**	**100**	**70**	**24**	**102**	**20**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0
8	Moduły praktyk specjalnościowych	160	2	10	148	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	10	148
	Ogółem praktyki	**960**	**8**	**40**	**912**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**2**	**10**	**148**
	OGÓŁEM:	**2046**				**190**			**198**			**472**			**378**			**502**			**306**		

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	23	0	0	8	9	3	3
Ogółem bez praktyk		**142**	**30**	**30**	**16**	**25**	**18**	**23**
7	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
Ogółem praktyki		**38**	**0**	**0**	**13**	**6**	**13**	**6**
OGÓŁEM:		**180**	**30**	**30**	**29**	**31**	**31**	**29**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**900**
Liczba godzin zajęć e-learningowych i projektów	**234**
Liczba godzin praktyk w Instytucji	**912**
Łączna liczba godzin w programie	**2046**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Zarządzanie zespołami operacyjnymi IT*
Stopień kształcenia: studia pierwszego stopnia
Forma studiów: niestacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-BEZFIZINF-3	Bezpieczeństwo fizyczne, środowiskowe i infrastruktury	O	3	30	14	16	0							14	16										
2	N1-00-AUDINCODP-4	Audyt incydentów i odporności	O	3	18	0	18	0											18							
3	N1-00-TESTPENME-3	Testy penetracyjne i metody ofensywne	O	3	20	0	20	0								20										
4	N1-00-WSPSOCZESP-4	Współpraca SOC i zespołów ds. ryzyka	O	2	12	0	12	0											12							
5	N1-00-NARZMONIT-4	Narzędzia monitoringu i automatyzacji (SIEM i SOAR)	O	3	24	12	12	0										12	12							
6	N1-00-ANALSTROP-4	Analiza strat i utrzymanie ciągłości operacyjnej	O	3	12	0	12	0											12							
7	N1-00-TWSCENINC-5	Tworzenie scenariuszy reakcji na incydenty	O	3	22	0	12	10														12	10			
8	N1-00-ZARZSTRATK-6	Zarządzanie stresem w trakcie ataku	O	3	20	0	20	0																	20	
		RAZEM:		**23**	**158**	**26**	**122**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**14**	**36**	**0**	**12**	**54**	**0**	**0**	**12**	**10**	**0**	**20**	**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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148																2	10	148
2					0	0	0	0																		
3					0	0	0	0																		
4					0	0	0	0																		
		RAZEM:		**6**	**160**	**2**	**10**	**148**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**148**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																	
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6		
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	252	80	168	4	42	80	4	38	76	0	0	12	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	394	102	252	40	28	36	0	24	50	10	14	0	0	12	50	10	0	54	10	24	62	10
3	Moduły przygotowania pracy dyplomowej	54	0	54	0	0	0	0	0	0	0	0	0	0	0	12	0	0	18	0	0	24	0
4	Moduły kształcenia językowego	228	0	48	180	0	0	0	0	0	0	0	16	60	0	16	60	0	16	60	0	0	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	158	26	122	10	0	0	0	0	0	0	14	36	0	12	54	0	0	12	10	0	20	0
	Ogółem bez praktyk	**1086**	**208**	**644**	**234**	**70**	**116**	**4**	**62**	**126**	**10**	**28**	**64**	**60**	**24**	**132**	**70**	**0**	**100**	**80**	**24**	**106**	**10**
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0
8	Moduły praktyk specjalnościowych	160	2	10	148	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	10	148
	Ogółem praktyki	**960**	**8**	**40**	**912**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**2**	**10**	**148**
	OGÓŁEM:	**2046**				**190**			**198**			**472**			**386**			**500**			**300**		

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	23	0	0	6	11	3	3
	Ogółem bez praktyk	**142**	**30**	**30**	**14**	**27**	**18**	**23**
7	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
	Ogółem praktyki	**38**	**0**	**0**	**13**	**6**	**13**	**6**
	OGÓŁEM:	**180**	**30**	**30**	**27**	**33**	**31**	**29**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**900**
Liczba godzin zajęć e-learningowych i projektów	**234**
Liczba godzin praktyk w Instytucji	**912**
Łączna liczba godzin w programie	**2046**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Cyberhigiena i edukacja informacyjna*
Stopień kształcenia: studia pierwszego stopnia
Forma studiów: niestacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	N1-00-CYBERGRSP-3	Cyberbezpieczeństwo wybranych grup społecznych - modele zarządzania ryzykiem	O	3	30	14	16	0							14	16										
2	N1-00-STRZARRLUD-4	Strategie zarządzania ryzykiem ludzkim w organizacjach	O	3	18	0	18	0											18							
3	N1-00-BEZUZALTE-3	Bezpieczeństwo organizacji wobec uzależnień technologicznych	O	3	20	0	20	0								20										
4	N1-00-TECHEDU-4	Technologie wspierające edukację i monitorowanie efektywności	O	2	12	0	12	0											12							
5	N1-00-PROJNARE-4	Projektowanie i zarządzanie narzędziami edukacyjnymi	O	3	24	12	12	0										12	12							
6	N1-00-PROJELEARN-4	Projektowanie interaktywnych szkoleń i e-learningu - aspekty wdrożeniowe	O	3	12	0	12	0											12							
7	N1-00-WDZPSYCH-5	Wspieranie zdrowia psychicznego pracowników w środowisku cyfrowym	O	3	22	0	12	10														12	10			
8	N1-00-METODEFEK-6	Metody badania efektywności programów edukacyjnych bezpieczeństwa i zarządzania jakością edukacji	O	3	20	0	20	0																	20	
		RAZEM:		**23**	**158**	**26**	**122**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**14**	**36**	**0**	**12**	**54**	**0**	**0**	**12**	**10**	**0**	**20**	**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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	N1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148																2	10	148
2					0	0	0	0																		
3					0	0	0	0																		
4					0	0	0	0																		
		RAZEM:		**6**	**160**	**2**	**10**	**148**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**148**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																				
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6					
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	252	80	168	4	42	80	4	38	76	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	394	102	252	40	28	36	0	24	50	10	14	0	0	12	50	10	0	54	10	24	62	10			
3	Moduły przygotowania pracy dyplomowej	54	0	54	0	0	0	0	0	0	0	0	0	0	0	12	0	0	18	0	0	24	0			
4	Moduły kształcenia językowego	228	0	48	180	0	0	0	0	0	0	0	16	60	0	16	60	0	16	60	0	0	0			
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
6	Moduły kształcenia specjalnościowego	158	26	122	10	0	0	0	0	0	0	14	36	0	12	54	0	0	12	10	0	20	0			
	Ogółem bez praktyk	**1086**	**208**	**644**	**234**	**70**	**116**	**4**	**62**	**126**	**10**	**28**	**64**	**60**	**24**	**132**	**70**	**0**	**100**	**80**	**24**	**106**	**10**			

	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0
8	Moduły praktyk specjalnościowych	160	2	10	148	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	10	148
	Ogółem praktyki	**960**	**8**	**40**	**912**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**2**	**10**	**148**
	OGÓŁEM:	**2046**				**190**			**198**			**472**			**386**			**500**			**300**		

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	23	0	0	6	11	3	3
	Ogółem bez praktyk	**142**	**30**	**30**	**14**	**27**	**18**	**23**
7	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
	Ogółem praktyki	**38**	**0**	**0**	**13**	**6**	**13**	**6**
	OGÓŁEM:	**180**	**30**	**30**	**27**	**33**	**31**	**29**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**900**
Liczba godzin zajęć e-learningowych i projektów	**234**
Liczba godzin praktyk w Instytucji	**912**
Łączna liczba godzin w programie	**2046**

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

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	60	30	30	0	30	30																
2	S1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	60	30	30	0	30	30																
3	S1-00-PODSTEKON-2	Podstawy ekonomii	O	4	50	30	20	0				30	20													
4	S1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	60	30	30	0				30	30													
5	S1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	60	30	30	0	30	30																
6	S1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	30	0	30	0					30													
7	S1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	50	30	20	0				30	20													
8	S1-00-TECHNINFO-1	Technologie informatyczne	O	3	30	0	30	0		30																
9	S1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	16	0	16	0		16																
10	S1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	16	0	16	0					16													
11	S1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	16	0	16	0								16										
12	S1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4			4															
		RAZEM:		**40**	**452**	**180**	**268**	**4**	**90**	**136**	**4**	**90**	**116**	**0**	**0**	**16**	**0**	**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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	60	30	30	0	30	30																
2	S1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami (Gantt, asana, kanban)	O	4	40	0	30	10					30	10												
3	S1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	36	0	36	0																	36	
4	S1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	50	30	20	0				30	20													
5	S1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	50	30	20	0				30	20													
6	S1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	26	0	26	0																	26	
7	S1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	46	0	36	10														36	10			
8	S1-00-OSINTANAL-1	Biały wywiad (OSINT) i analiza informacji	E	5	60	30	30	0	30	30																
9	S1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	50	20	20	10																20	20	10
10	S1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	50	30	20	0										30	20							
11	S1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	30	0	30	0											30							
12	S1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	30	0	30	0														30				
13	S1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	50	20	30	0																20	30	
14	S1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	20	20	0	0							20											
15	S1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	30	0	20	10											20	10						
16	S1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	20	0	20	0														20				
		RAZEM:		**55**	**648**	**210**	**398**	**40**	**60**	**60**	**0**	**60**	**70**	**10**	**20**	**0**	**0**	**30**	**70**	**10**	**0**	**86**	**10**	**40**	**112**	**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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-METBAD-4	Metodologia badań z elementami statystyki	O	2	20	0	20	0											20							
2	S1-00-SEMDYP1-5	Seminarium I	O	3	30	0	30	0														30				
3	S1-00-SEMDYP2-6	Seminarium II	O	7	40	0	40	0																	40	
		RAZEM:		**12**	**90**	**0**	**90**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**20**	**0**	**0**	**30**	**0**	**0**	**40**	**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			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	84	0	24	60								24	60									
2	S1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	84	0	24	60											24	60						
3	S1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	84	0	24	60														24	60			
		RAZEM:		**12**	**252**	**0**	**72**	**180**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**24**	**60**	**0**	**24**	**60**	**0**	**24**	**60**	**0**	**0**	**0**

Moduły kształcenia w zakresie kultury fizycznej

Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Semestr																	
									sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6		
					ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-WF1-3	Wychowanie fizyczne I	ZAL	0	30	0	30	0								30										
2	S1-00-WF2-4	Wychowanie fizyczne II	ZAL	0	30	0	30	0											30							
					0	0	0	0																		
		RAZEM:		**0**	**60**	**0**	**60**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**30**	**0**	**0**	**30**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308							2	10	308									
2	S1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148										2	10	148						
3	S1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I (wybieralna)	ZAL	13	320	2	10	308													2	10	308			
4					0	0	0	0																		
		RAZEM:		**32**	**800**	**6**	**30**	**764**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**0**	**0**	**0**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																				
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6					
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	452	180	268	4	90	136	4	90	116	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	648	210	398	40	60	60	0	60	70	10	20	0	0	30	70	10	0	86	10	40	112	10			
3	Moduły przygotowania pracy dyplomowej	90	0	90	0	0	0	0	0	0	0	0	0	0	0	20	0	0	30	0	0	40	0			
4	Moduły kształcenia językowego	252	0	72	180	0	0	0	0	0	0	0	24	60	0	24	60	0	24	60	0	0	0			
5	Moduły kształcenia w zakresie kultury fizycznej	60	0	60	0	0	0	0	0	0	0	0	30	0	0	30	0	0	0	0	0	0	0			
	Razem bez modułu praktyk kierunkowych:	**1502**	**390**	**888**	**224**	**150**	**196**	**4**	**150**	**186**	**10**	**20**	**70**	**60**	**30**	**144**	**70**	**0**	**140**	**70**	**40**	**152**	**10**			
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.			
6	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0			
	RAZEM z modułem praktyk kierunkowych:	**2302**				**350**			**346**			**470**			**404**			**530**			**202**					

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
	RAZEM:	**151**	**30**	**30**	**21**	**22**	**28**	**20**
	Moduł kształcenia specjalnościowego:	*29*	*0*	*0*	*9*	*8*	*2*	*10*
	OGÓŁEM:	**180**	**30**	**30**	**30**	**30**	**30**	**30**
	Dopuszczalny deficyt punktowy po semetrze:		-5	-5	-5	-5	-5	-5

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Biały wywiad w zarządzaniu cyberbezpieczeństwem*
Stopień kształcenia: studia pierwszego stopnia
Forma studiów: stacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-PSYCHSLED-3	Psychologia śledcza i profilowanie w cyberprzestrzeni	O	3	36	0	36	0								36										
2	S1-00-PSYCHPOZN-4	Psychologia poznawcza w wywiadzie i analizie danych	O	3	36	0	36	0											36							
3	S1-00-PSYCHPOZAN-3	Zarządzanie stresem i efektywność pracy	O	3	36	0	36	0								36										
4	S1-00-ZRODANOS-3	Źródła danych dla białego wywiadu	O	2	20	20	0	0							20											
5	S1-00-OSINTBEH-4	OSINT i analiza behawioralna	O	3	36	0	36	0											36							
6	S1-00-NARZAISLU-4	Narzędzia i AI w służbie białego wywiadu	O	3	36	0	36	0											36							
7	S1-00-ANALINFOR-5	Analiza informacji i raportowanie	O	3	44	20	24	0													20	24				
8	S1-00-DSGTHCYB-6	Design Thinking w cyberbezpieczenieństwie	O	3	40	0	30	10																	30	10
		RAZEM:		**23**	**284**	**40**	**234**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**20**	**72**	**0**	**0**	**108**	**0**	**20**	**24**	**0**	**0**	**30**	**10**

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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148																2	10	148
2					0	0	0	0																		
3					0	0	0	0																		
4					0	0	0	0																		
		RAZEM:		**6**	**160**	**2**	**10**	**148**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**148**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																				
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6					
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	452	180	268	4	90	136	4	90	116	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	648	210	398	40	60	60	0	60	70	10	20	0	0	30	70	10	0	86	10	40	112	10			
3	Moduły przygotowania pracy dyplomowej	90	0	90	0	0	0	0	0	0	0	0	0	0	0	20	0	0	30	0	0	40	0			
4	Moduły kształcenia językowego	252	0	72	180	0	0	0	0	0	0	0	24	60	0	24	60	0	24	60	0	0	0			
5	Moduły kształcenia w zakresie kultury fizycznej	60	0	60	0	0	0	0	0	0	0	0	30	0	0	30	0	0	0	0	0	0	0			
6	Moduły kształcenia specjalnościowego	284	40	234	10	0	0	0	0	0	0	20	72	0	0	108	0	20	24	0	0	30	10			
	Ogółem bez praktyk	**1786**	**430**	**1122**	**234**	**150**	**196**	**4**	**150**	**186**	**10**	**40**	**142**	**60**	**30**	**252**	**70**	**20**	**164**	**70**	**40**	**182**	**20**			
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.			
7	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0			
8	Moduły praktyk specjalnościowych	160	2	10	148	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	10	148			
	Ogółem praktyki	**960**	**8**	**40**	**912**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**2**	**10**	**148**			
	OGÓŁEM:	**2746**				**350**			**346**			**562**			**512**			**574**			**402**					

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	23	0	0	8	9	3	3
	Ogółem bez praktyk	**142**	**30**	**30**	**16**	**25**	**18**	**23**
7	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
	Ogółem praktyki	**38**	**0**	**0**	**13**	**6**	**13**	**6**
	OGÓŁEM:	**180**	**30**	**30**	**29**	**31**	**31**	**29**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**1600**
Liczba godzin zajęć e-learningowych i projektów	**234**
Liczba godzin praktyk w Instytucji	**912**
Łączna liczba godzin w programie	**2746**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Zarządzanie zespołami operacyjnymi IT*
Stopień kształcenia: studia pierwszego stopnia
Forma studiów: stacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-BEZFIZINF-3	Bezpieczeństwo fizyczne, środowiskowe i infrastruktury	O	3	40	20	20	0							20	20										
2	S1-00-AUDINCODP-4	Audyt incydentów i odporności	O	3	36	0	36	0											36							
3	S1-00-TESTPENME-3	Testy penetracyjne i metody ofensywne	O	3	36	0	36	0								36										
4	S1-00-WSPSOCZESP-4	Współpraca SOC i zespołów ds. ryzyka	O	2	20	0	20	0											20							
5	S1-00-NARZMONIT-4	Narzędzia monitoringu i automatyzacji (SIEM i SOAR)	O	3	40	20	20	0										20	20							
6	S1-00-ANALSTROP-4	Analiza strat i utrzymanie ciągłości operacyjnej	O	3	36	0	36	0											36							
7	S1-00-TWSCENINC-5	Tworzenie scenariuszy reakcji na incydenty	O	3	40	0	30	10														30	10			
8	S1-00-ZARZSTRATK-6	Zarządzanie stresem w trakcie ataku	O	3	36	0	36	0																	36	
RAZEM:				**23**	**284**	**40**	**234**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**20**	**56**	**0**	**20**	**112**	**0**	**0**	**30**	**10**	**0**	**36**	**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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148																2	10	148
2					0	0	0	0																		
3					0	0	0	0																		
4					0	0	0	0																		
RAZEM:				**6**	**160**	**2**	**10**	**148**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**148**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																				
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6					
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	452	180	268	4	90	136	4	90	116	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	648	210	398	40	60	60	0	60	70	10	20	0	0	30	70	10	0	86	10	40	112	10			
3	Moduły przygotowania pracy dyplomowej	90	0	90	0	0	0	0	0	0	0	0	0	0	0	20	0	0	30	0	0	40	0			
4	Moduły kształcenia językowego	252	0	72	180	0	0	0	0	0	0	0	24	60	0	24	60	0	24	60	0	0	0			
5	Moduły kształcenia w zakresie kultury fizycznej	60	0	60	0	0	0	0	0	0	0	0	30	0	0	30	0	0	0	0	0	0	0			
6	Moduły kształcenia specjalnościowego	284	40	234	10	0	0	0	0	0	0	20	56	0	20	112	0	0	30	10	0	36	0			
Ogółem bez praktyk		**1786**	**430**	**1122**	**234**	**150**	**196**	**4**	**150**	**186**	**10**	**40**	**126**	**60**	**50**	**256**	**70**	**0**	**170**	**80**	**40**	**188**	**10**			
Moduły praktyk		Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
7	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0			
8	Moduły praktyk specjalnościowych	160	2	10	148	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	10	148			
Ogółem praktyki		**960**	**8**	**40**	**912**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**2**	**10**	**148**			
OGÓŁEM:		**2746**				**350**			**346**			**546**			**536**			**570**			**398**					

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	23	0	0	6	11	3	3
	Ogółem bez praktyk	**142**	**30**	**30**	**14**	**27**	**18**	**23**
7	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
	Ogółem praktyki	**38**	**0**	**0**	**13**	**6**	**13**	**6**
	OGÓŁEM:	**180**	**30**	**30**	**27**	**33**	**31**	**29**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**1600**
Liczba godzin zajęć e-learningowych i projektów	**234**
Liczba godzin praktyk w Instytucji	**912**
Łączna liczba godzin w programie	**2746**

Wydział: Wydział Studiów Stosowanych we Wrocławiu
Kierunek: Zarządzanie cyberbezpieczeństwem
Moduł wybieralny: *Cyberhigiena i edukacja informacyjna*
Stopień kształcenia: studia pierwszego stopnia
Forma studiów: stacjonarne
Profil: praktyczny
Dyscyplina wiodąca: nauki o zarządzaniu i jakości - 60%
Dyscyplina uzupełniająca: bezpieczeństwo - 40%

Czas trwania: 6 semestrów
Obowiązuje od roku akademickiego: 2026/27

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			sem. 5			sem. 6		
					Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	S1-00-BEZFIZINF-3	Cyberbezpieczeństwo wybranych grup społecznych - modele zarządzania ryzykiem	O	3	40	20	20	0							20	20										
2	S1-00-AUDINCODP-4	Strategie zarządzania ryzykiem ludzkim w organizacjach	O	3	36	0	36	0											36							
3	S1-00-TESTPENME-3	Bezpieczeństwo organizacji wobec uzależnień technologicznych	O	3	36	0	36	0								36										
4	S1-00-WSPSOCZESP-4	Technologie wspierające edukację i monitorowanie efektywności	O	2	20	0	20	0											20							
5	S1-00-NARZMONIT-4	Projektowanie i zarządzanie narzędziami edukacyjnymi	O	3	40	20	20	0										20	20							
6	S1-00-ANALSTROP-4	Projektowanie interaktywnych szkoleń i e-learningu - aspekty wdrożeniowe	O	3	36	0	36	0											36							
7	S1-00-TWSCENINC-5	Wspieranie zdrowia psychicznego pracowników w środowisku cyfrowym	O	3	40	0	30	10														30	10			
8	S1-00-ZARZSTRATK-6	Metody badania efektywności programów edukacyjnych bezpieczeństwa i zarządzania jakością edukacji	O	3	36	0	36	0																	36	
		RAZEM:		**23**	**284**	**40**	**234**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**20**	**56**	**0**	**20**	**112**	**0**	**0**	**30**	**10**	**0**	**36**	**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			sem. 5			sem. 6		
					Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.
1	S1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148																2	10	148
2					0	0	0	0																		
3					0	0	0	0																		
4					0	0	0	0																		
		RAZEM:		**6**	**160**	**2**	**10**	**148**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**148**

Podsumowanie

Godziny

Lp.	Moduły	Liczba godz.				Semestr																				
						sem. 1			sem. 2			sem. 3			sem 4			sem. 5			sem. 6					
		Ogół.	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e	wyk.	ćw.	p/e
1	Moduły kształcenia podstawowego	452	180	268	4	90	136	4	90	116	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Moduły kształcenia kierunkowego	648	210	398	40	60	60	0	60	70	10	20	0	0	30	70	10	0	86	10	40	112	10			
3	Moduły przygotowania pracy dyplomowej	90	0	90	0	0	0	0	0	0	0	0	0	0	0	20	0	0	30	0	0	40	0			
4	Moduły kształcenia językowego	252	0	72	180	0	0	0	0	0	0	0	24	60	0	24	60	0	24	60	0	0	0			
5	Moduły kształcenia w zakresie kultury fizycznej	60	0	60	0	0	0	0	0	0	0	0	30	0	0	30	0	0	0	0	0	0	0			
6	Moduły kształcenia specjalnościowego	284	40	234	10	0	0	0	0	0	0	20	56	0	20	112	0	0	30	10	0	36	0			
	Ogółem bez praktyk	**1786**	**430**	**1122**	**234**	**150**	**196**	**4**	**150**	**186**	**10**	**40**	**126**	**60**	**50**	**256**	**70**	**0**	**170**	**80**	**40**	**188**	**10**			
	Moduły praktyk	Ogół.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.	WP	EW	prak.			
7	Moduły praktyk kierunkowych	800	6	30	764	0	0	0	0	0	0	2	10	308	2	10	148	2	10	308	0	0	0			
	Ogółem praktyki	**960**	**8**	**40**	**912**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**10**	**308**	**2**	**10**	**148**	**2**	**10**	**308**	**2**	**10**	**148**			
	OGÓŁEM:	**2746**				**350**			**346**			**546**			**536**			**570**			**398**					

Punkty ECTS

Lp.		Liczba punktów	Semestr					
			sem. 1	sem. 2	sem. 3	sem 4	sem. 5	sem. 6
1	Moduły kształcenia podstawowego	40	20	18	2	0	0	0
2	Moduły kształcenia kierunkowego	55	10	12	2	10	8	13
3	Moduły przygotowania pracy dyplomowej	12	0	0	0	2	3	7
4	Moduły kształcenia językowego	12	0	0	4	4	4	0
5	Moduły kształcenia w zakresie kultury fizycznej	0	0	0	0	0	0	0
6	Moduły kształcenia specjalnościowego	23	0	0	6	11	3	3
		142	**30**	**30**	**14**	**27**	**18**	**23**
7	Moduły praktyk kierunkowych	32	0	0	13	6	13	0
8	Moduły praktyk specjalnościowych	6	0	0	0	0	0	6
	Ogółem praktyki	**38**	**0**	**0**	**13**	**6**	**13**	**6**
	OGÓŁEM:	**180**	**30**	**30**	**27**	**33**	**31**	**29**

Liczba godzin bez praktyk w Instytucji, zajęć e-learningowych i projektów	**1600**
Liczba godzin zajęć e-learningowych i projektów	**234**
Liczba godzin praktyk w Instytucji	**912**
Łączna liczba godzin w programie	**2746**

Macierz efektów uczenia się

Uczelnia:	**Uniwersytet DSW Ideis**
Wydział:	**Studiów Stosowanych we Wrocławiu**
Kierunek:	**Zarządzanie cyberbezpieczeństwem**
Moduł kształcenia wybieralnego / w zakresie	***Cyberhigiena i edukacja informacyjna***
Stopień kształcenia:	**Licencjat (1 stopień)**
Profil:	**Praktyczny**
Czas trwania	**6 semestrów**
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)								
				Wprowadzenie do cyberbezpieczeństwa	Podstawy zarządzania	Podstawy ekonomii	Psychologia cyberbezpieczeństwa	Logika i krytyczne myślenie	Etyka i prywatność danych	Aspekty prawne i regulacje w cyberbezpieczeństwie	Technologie informatyczne	Kompetencje przyszłości I	Kompetencje przyszłości II	Kompetencje przyszłości III	Szkolenie wstępne z zakresu BHP	Systemy ICT w cyberbezpieczeństwie	Cyfrowe zarządzanie projektami (Gantt, asana, kanban)	Zarządzanie ryzykiem w cyberprzestrzeni	Organizacja i zarządzanie	Cyberbezpieczeństwo operacyjne (wprow. narz. SIEM i SOAR, SOC)	Warsztat pracy z grupą	Modelowanie cyberzagrożeń	Biały wywiad (OSINT) i analiza informacji	Testowanie i audyty cyberbezpieczeństwa	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	Analiza i zarządzanie podatnościami	Kultura bezpieczeństwa organizacji	Praktyki zarządzania incydentami	Podstawy Threat Intelligence	Socjologia dezinformacji i wojen informacyjnych	Role i uprawnienia w bezpieczeństwie informacji	Język obcy I (j.angielski, j.niemiecki)	Język obcy II (j.angielski, j.niemiecki)	Język obcy III (j.angielski, j.niemiecki)	Metodologia badań	Seminarium I	Seminarium II	Praktyka zawodowa ogólna I	Praktyka zawodowa ogólna II	Praktyka zawodowa kierunkowa I	Praktyka zawodowa kierunkowa II	Cyberbezpieczeństwo wybranych grup społecznych - modele zarządzania ryzykiem	Strategie zarządzania ryzykiem ludzkim w organizacjach	Bezpieczeństwo organizacji wobec zależności technologicznych	Technologie wspierające edukację i monitorowanie efektywności	Projektowanie i zarządzanie narzędziami edukacyjnymi	Projektowanie interaktywnych szkoleń i e-learningu - aspekty wdrożeniowe	Wspieranie zdrowia psychicznego pracowników w środowisku cyfrowym	Metody badania efektywności programów edukacyjnych bezpieczeństwa i zarządzania
WIEDZA absolwent zna i rozumie:				**3**	**3**	**2**	**2**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**3**	**3**	**3**	**2**	**3**	**1**	**3**	**3**	**2**	**3**	**4**	**2**	**3**	**3**	**0**	**0**	**0**	**0**	**1**	**0**	**2**	**2**	**2**	**2**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**
W zaawansowanym stopniu zna i opisuje kluczowe koncepcje zarządzania i cyberbezpieczeństwa oraz ich powiązania z funkcjonowaniem organizacji	ZCYB_I_W01	PRK6_WG	**6**	x	x	x																														x				x							x
W zaawansowanym stopniu zna funkcje zarządzania oraz rozumie ich zastosowanie w praktyce organizacji	ZCYB_I_W02	PRK6_WG	**8**		x	x											x	x	x	x							x									x										
W zaawansowanym stopniu zna elementy architektury systemów ICT oraz narzędzia wspierające zapewnienie bezpieczeństwa organizacji	ZCYB_I_W03	PRK6_WG	**6**	x							x					x				x		x																			x						
W zaawansowanym stopniu zna i klasyfikuje rodzaje zagrożeń, podatności i incydentów w cyberprzestrzeni oraz ich wpływ na funkcjonowanie organizacji	ZCYB_I_W04	PRK6_WG	**8**	x													x			x		x				x	x	x										x								
W zaawansowanym stopniu zna i rozumie istotę strategii zarządzania bezpieczeństwem informacji, w tym procesy analizy ryzyka, audytu bezpieczeństwa oraz zarządzania ciągłością działania	ZCYB_I_W05	PRK6_WK	**9**															x	x					x	x				x						x					x	x						
W zaawansowanym stopniu zna modele organizacyjne oraz rozumie zasady funkcjonowania zespołów operacyjnych w kontekście bezpieczeństwa	ZCYB_I_W06	PRK6_WK	**3**		x																x				x																				
W zaawansowanym stopniu zna normy, standardy i przepisy prawne wpływające na procesy zarządzania bezpieczeństwem informacji	ZCYB_I_W07	PRK6_WG	**7**						x	x					x									x	x				x									x								
W zaawansowanym stopniu zna psychologiczne i społeczne aspekty cyberzagrożeń	ZCYB_I_W08	PRK6_WG	**7**				x														x					x			x														x		
W zaawansowanym stopniu zna metody i techniki zarządzania projektami i procesami w obszarze bezpieczeństwa informacji	ZCYB_I_W09	PRK6_WG	**5**														x			x																						x	x				
W zaawansowanym stopniu zna i rozumie znaczenie zarządzania wiedzą i budowania kultury bezpieczeństwa w organizacji	ZCYB_I_W10	PRK6_WG	**9**																							x																x	x	x	x	x	x	x
W zaawansowanym stopniu zna techniki monitorowania i analizy zagrożeń (SIEM/SOAR, OSINT) oraz ich zastosowanie w praktyce organizacyjnej	ZCYB_I_W11	PRK6_WK	**5**								x					x			x				x						x																	
W zaawansowanym stopniu zna zasady ochrony informacji, danych osobowych, prywatności oraz etyki w środowisku cyfrowym	ZCYB_I_W12	PRK6_WK	**5**							x					x								x				x																			
W zaawansowanym stopniu zna metody projektowania scenariuszy reakcji na incydenty oraz planów ciągłości działania organizacji	ZCYB_I_W13	PRK6_WK	**4**																	x			x			x																	x				
W zaawansowanym stopniu zna zasady rozwoju kompetencji zawodowych i uczenia się przez całe życie w obszarze zarządzania cyberbezpieczeństwem	ZCYB_I_W14	PRK6_WK	**7**									x	x	x																													x	x				x
W zaawansowanym stopniu zna i rozumie znaczenie społecznej odpowiedzialności i konsekwencje działań związanych z cyberbezpieczeństwem	ZCYB_I_W15	PRK6_WK	**8**				x	x	x																	x																x		x				
UMIEJĘTNOŚCI absolwent potrafi:				**1**	**1**	**0**	**1**	**3**	**3**	**2**	**2**	**3**	**3**	**3**	**2**	**2**	**3**	**3**	**3**	**3**	**4**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**2**	**1**	**1**	**1**	**0**	**3**	**3**	**2**	**2**	**2**	**2**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**
Umie analizować i oceniać problemy organizacyjne oraz zagrożenia cybernetyczne, proponując adekwatne rozwiązania zarządcze i techniczne	ZCYB_I_U01	PRK6_UW	**9**					x									x				x		x						x												x	x					x
Umie prowadzić skuteczną komunikację oraz koordynować działania w sytuaciach kryzysowych	ZCYB_I_U02	PRK6_UK	**5**														x				x					x		x																	x		
Umie wykorzystywać techniki OSINT i narzędzia analityczne w identyfikacji podatności i analizie ryzyka	ZCYB_I_U03	PRK6_UW	**7**	x							x					x				x		x						x																			
Umie projektować i realizować działania rozwijające i wspierające kulturę bezpieczeństwa w organizacji	ZCYB_I_U04	PRK6_UO	**8**				x														x					x																x	x	x				
Umie przeprowadzać audyty i testy bezpieczeństwa oraz opracowywać stosowną dokumentację zgodnie z obowiązującymi standardami	ZCYB_I_U05	PRK6_UW	**5**					x		x														x	x																		x					
Umie stosować narzędzia do monitoringu oraz analizy cyberzagrożeń (SIEM, SOAR, OSINT) i oceniać efektywność zabezpieczeń	ZCYB_I_U06	PRK6_UW	**6**								x					x				x				x		x																	x					
Umie opracowywać, wdrażać i aktualizować procedury reagowania na incydenty bezpieczeństwa informacji	ZCYB_I_U07	PRK6_UW	**4**																		x				x																			x					
Umie stosować strategie zarządzania zmianą i dostosowywać działania organizacyjne do dynamicznego otoczenia technologicznego.	ZCYB_I_U08	PRK6_UW	**6**															x	x									x																x		x				
Umie planować, organizować i kontrolować zadania zespołów oraz zarządzać projektami w obszarze bezpieczeństwa informacji	ZCYB_I_U09	PRK6_UO	**5**		x												x		x																								x					
Umie planować i realizować działania zapewniające ciągłość działania oraz organizować reakcje awaryjne	ZCYB_I_U10	PRK6_UW	**5**												x															x													x		x				
Umie stosować przepisy prawne, normy branżowe i zasady etyki w praktyce zawodowej w zakresie zarządzania bezpieczeństwem	ZCYB_I_U11	P6S_UW	**6**						x	x					x										x				x													x					

Umie efektywnie współpracować w zespołach interdyscyplinarnych oraz komunikować się z różnymi grupami interesariuszy	ZCYB_I_U12	PRK6_UK	**5**									x	x	x			x				x																												
Umie przygotowywać raporty i prezentacje opisujące stany i incydenty bezpieczeństwa, rekomendując działania zaradcze	ZCYB_I_U13	PRK6_UK	**7**						x														x													x	x								x		x		x
Umie efektywnie organizować pracę własną i zespołową, delegować zadania i działać pod presją czasu	ZCYB_I_U14	P6S_UO	**9**									x	x	x			x		x		x																	x						x				x	
Umie planować i wdrażać działania podnoszące świadomość i kulturę bezpieczeństwa w organizacji	ZCYB_I_U15	P6S_UO	**4**																		x						x														x		x						
Umie posługiwać się językiem obcym (na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego) w zakresie zarządzania i cyberbezpieczeństwa, w tym w środowisku pracy	ZCYB_I_U16	PRK6_UK	**8**																		x		x							x		x	x	x		x	x												
Umie krytycznie oceniać i aktualizować własną wiedzę oraz doskonalić kompetencje zawodowe w obszarze cyberbezpieczeństwa	ZCYB_I_U17	PRK6_UU	**9**					x	x			x	x	x																						x	x								x				x
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:				**2**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**3**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
Jest gotów do współpracy w zespołach oraz skutecznej komunikacji z różnymi grupami interesariuszy w środowisku zawodowym.	ZCYB_I_K01	PRK6_KR	**12**		x						x		x				x		x		x					x	x	x			x							x									x		
Jest gotów do uwzględniania konsekwencji społecznych, prawnych i etycznych działań w zakresie zarządzania cyberbezpieczeństwem	ZCYB_I_K02	P6S_KO	**15**	x			x		x	x				x	x			x		x		x			x					x									x	x			x					x	
Jest gotów do przestrzegania zasad etyki zawodowej i promowania kultury bezpieczeństwa informacji	ZCYB_I_K03	PRK6_KO	**10**		x				x	x		x			x									x	x						x							x						x					
Jest gotów do krytycznej samooceny własnych kompetencji i planowania rozwoju zawodowego w obszarze zarządzania cyberbezpieczeństwem	ZCYB_I_K04	PRK6_KK	**8**					x			x								x									x							x	x	x												x
Jest gotów do korzystania z wiedzy ekspertów i współpracy specjalistycznej w celu rozwiązywania problemów poznawczych i praktycznych	ZCYB_I_K05	PRK6_KK	**10**	x		x		x								x				x			x						x						x										x				x
Jest gotów do podejmowania inicjatyw i działań podnoszących poziom bezpieczeństwa informacji i kultury organizacyjnej, w sposób przedsiębiorczy i innowacyjny	ZCYB_I_K06	PRK6_KR	**12**										x				x	x								x	x			x									x	x	x		x			x	x		
Jest gotów do otwartego przyjmowania krytyki i dążenia do stałego rozwoju osobistego oraz zespołowego	ZCYB_I_K07	PRK6_KR	**10**				x					x										x										x	x	x		x						x		x				x	
Jest gotów do kształtowania proaktywnej postawy w dzieleniu się wiedzą i doświadczeniami	ZCYB_I_K08	PRK6_KO	**12**														x				x		x				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 zespołami operacyjnymi IT***
Stopień kształcenia: **Licencjat (I stopień)**
Profil: **Praktyczny**
Czas trwania **6 semestrów**
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)							
				Wprowadzenie do cyberbezpieczeństwa	Podstawy zarządzania	Podstawy ekonomii	Psychologia cyberbezpieczeństwa	Logika i krytyczne myślenie	Etyka i prywatność danych	Aspekty prawne i regulacje w cyberbezpieczeństwie	Technologie informatyczne	Kompetencje przyszłości I	Kompetencje przyszłości II	Kompetencje przyszłości III	Szkolenie wstępne z zakresu BHP	Systemy ICT w cyberbezpieczeństwie	Cyfrowe zarządzanie projektami (Gantt, asana, kanban)	Zarządzanie ryzykiem w cyberprzestrzeni	Organizacja i zarządzanie	Cyberbezpieczeństwo operacyjne (wprow. narz. SIEM i SOAR, SOC)	Warsztat pracy z grupą	Modelowanie cyberzagrożeń	Biały wywiad (OSINT) i analiza informacji	Testowanie i audyty cyberbezpieczeństwa	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	Analiza i zarządzanie podatnościami	Kultura bezpieczeństwa organizacji	Praktyki zarządzania incydentami	Podstawy Threat Intelligence	Socjologia dezinformacji i wojen informacyjnych	Role i uprawnienia w bezpieczeństwie informacji	Język obcy I (j.angielski, j.niemiecki)	Język obcy II (j.angielski, j.niemiecki)	Język obcy III (j.angielski, j.niemiecki)	Metodologia badań	Seminarium I	Seminarium II	Praktyka zawodowa ogólna I	Praktyka zawodowa ogólna II	Praktyka zawodowa kierunkowa I	Praktyka zawodowa kierunkowa II	Bezpieczeństwo fizyczne, środowiskowe i infrastruktury	Audyt incydentów i odpomości	Testy penetracyjne i metody ofensywne	Współpraca SOC i zespołów ds. ryzyka	Narzędzia monitoringu i autom. (SIEM i SOAR)	Analiza strat i utrzymanie ciągłości operacyjnej	Tworzenie scenariuszy reakcji na incydenty	Zarządzanie stresem w trakcie ataku
WIEDZA **absolwent zna i rozumie:**				**3**	**3**	**2**	**2**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**3**	**3**	**3**	**2**	**3**	**1**	**3**	**3**	**2**	**3**	**4**	**2**	**3**	**3**	**0**	**0**	**0**	**0**	**1**	**0**	**2**	**2**	**2**	**2**	**3**	**3**	**2**	**3**	**3**	**3**	**2**	**2**
W zaawansowanym stopniu zna i opisuje kluczowe koncepcje zarządzania i cyberbezpieczeństwa oraz ich powiązania z funkcjonowaniem organizacji	ZCYB_I_W01	PRK6_WG	**5**	x	x	x																														x						x				
W zaawansowanym stopniu zna funkcje zarządzania oraz rozumie ich zastosowanie w praktyce organizacji	ZCYB_I_W02	PRK6_WG	**8**		x	x											x	x	x	x							x									x										
W zaawansowanym stopniu zna elementy architektury systemów ICT oraz narzędzia wspierające zapewnienie bezpieczeństwa organizacji	ZCYB_I_W03	PRK6_WG	**8**	x							x					x				x		x																			x		x		x			
W zaawansowanym stopniu zna i klasyfikuje rodzaje zagrożeń, podatności i incydentów w cyberprzestrzeni oraz ich wpływ na funkcjonowanie organizacji	ZCYB_I_W04	PRK6_WG	**11**	x														x				x				x		x	x	x											x	x			x			
W zaawansowanym stopniu zna i rozumie istotę strategii zarządzania bezpieczeństwem informacji, w tym procesy analizy ryzyka, audytu bezpieczeństwa oraz zarządzania ciągłością działania	ZCYB_I_W05	PRK6_WK	**11**															x	x					x	x					x					x							x		x		x	x	
W zaawansowanym stopniu zna modele organizacyjne oraz rozumie zasady funkcjonowania zespołów operacyjnych w kontekście bezpieczeństwa	ZCYB_I_W06	PRK6_WK	**4**		x														x						x																	x				
W zaawansowanym stopniu zna normy, standardy i przepisy prawne wpływające na procesy zarządzania bezpieczeństwem informacji	ZCYB_I_W07	PRK6_WG	**7**						x	x					x									x	x					x									x							
W zaawansowanym stopniu zna psychologiczne i społeczne aspekty cyberzagrożeń	ZCYB_I_W08	PRK6_WG	**5**				x												x								x																		x
W zaawansowanym stopniu zna metody i techniki zarządzania projektami i procesami w obszarze bezpieczeństwa informacji	ZCYB_I_W09	PRK6_WG	**3**														x			x																						x				
W zaawansowanym stopniu zna i rozumie znaczenie zarządzania wiedzą i budowania kultury bezpieczeństwa w organizacji	ZCYB_I_W10	PRK6_WG	**4**																																											x		x
W zaawansowanym stopniu zna techniki monitorowania i analizy zagrożeń (SIEM/SOAR, OSINT) oraz ich zastosowanie w praktyce organizacyjnej	ZCYB_I_W11	PRK6_WK	**8**								x					x			x				x					x															x	x	x		
W zaawansowanym stopniu zna zasady ochrony informacji, danych osobowych, prywatności oraz etyki w środowisku cyfrowym	ZCYB_I_W12	PRK6_WK	**5**							x					x									x					x																		
W zaawansowanym stopniu zna metody projektowania scenariuszy reakcji na incydenty oraz planów ciągłości działania organizacji	ZCYB_I_W13	PRK6_WK	**6**																	x				x																			x	x			x		
W zaawansowanym stopniu zna zasady rozwoju kompetencji zawodowych i uczenia się przez całe życie w obszarze zarządzania cyberbezpieczeństwem	ZCYB_I_W14	PRK6_WK	**4**									x	x	x																															x			
W zaawansowanym stopniu zna i rozumie znaczenie społecznej odpowiedzialności i konsekwencje działań związanych z cyberbezpieczeństwem	ZCYB_I_W15	PRK6_WK	**5**				x	x	x																x				x																		
UMIEJĘTNOŚCI **absolwent potrafi:**				**1**	**1**	**0**	**1**	**3**	**3**	**2**	**2**	**3**	**3**	**3**	**2**	**2**	**3**	**3**	**3**	**3**	**4**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**2**	**1**	**1**	**1**	**0**	**3**	**3**	**2**	**2**	**2**	**2**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**
Umie analizować i oceniać problemy organizacyjne oraz zagrożenia cybernetyczne, proponując adekwatne rozwiązania zarządcze i techniczne	ZCYB_I_U01	PRK6_UW	**9**					x										x				x		x					x												x			x	x		
Umie prowadzić skuteczną komunikację oraz koordynować działania w sytuacjach kryzysowych	ZCYB_I_U02	PRK6_UK	**7**															x				x					x		x																x		x	x
Umie wykorzystywać techniki OSINT i narzędzia analityczne w identyfikacji podatności i analizie ryzyka	ZCYB_I_U03	PRK6_UW	**9**	x							x					x				x			x			x																	x		x			
Umie projektować i realizować działania rozwijające i wspierające kulturę bezpieczeństwa w organizacji	ZCYB_I_U04	PRK6_UO	**3**				x															x					x																				
Umie przeprowadzać audyty i testy bezpieczeństwa oraz opracowywać stosowną dokumentację zgodnie z obowiązującymi standardami	ZCYB_I_U05	PRK6_UW	**8**					x		x														x	x																		x		x			
Umie stosować narzędzia do monitoringu oraz analizy cyberzagrożeń (SIEM, SOAR, OSINT) i oceniać efektywność zabezpieczeń	ZCYB_I_U06	PRK6_UW	**7**								x					x				x				x		x																		x	x			
Umie opracowywać, wdrażać i aktualizować procedury reagowania na incydenty bezpieczeństwa informacji	ZCYB_I_U07	PRK6_UW	**6**																	x				x																				x			x		
Umie stosować strategie zarządzania zmianą i dostosowywać działania organizacyjne do dynamicznego otoczenia technologicznego.	ZCYB_I_U08	PRK6_UW	**3**															x	x									x																				
Umie planować, organizować i kontrolować zadania zespołów oraz zarządzać projektami w obszarze bezpieczeństwa informacji	ZCYB_I_U09	PRK6_UO	**5**		x												x		x																									x					
Umie planować i realizować działania zapewniające ciągłość działania oraz organizować reakcje awaryjne	ZCYB_I_U10	PRK6_UW	**6**												x																													x			x		
Umie stosować przepisy prawne, normy branżowe i zasady etyki w praktyce zawodowej w zakresie zarządzania bezpieczeństwem	ZCYB_I_U11	P6S_UW	**7**						x	x					x									x																			x					
Umie efektywnie współpracować w zespołach interdyscyplinarnych oraz komunikować się z różnymi grupami interesariuszy	ZCYB_I_U12	PRK6_UK	**6**									x	x	x			x					x																							x				

Umie przygotowywać raporty i prezentacje opisujące stany i incydenty bezpieczeństwa, rekomendując działania zaradcze	ZCYB_I_U13	PRK6_UK	6						x														x													x	x											x	x
Umie efektywnie organizować pracę własną i zespołową, delegować zadania i działać pod presją czasu	ZCYB_I_U14	P6S_UO	7									x	x	x			x		x		x																	x											
Umie planować i wdrażać działania podnoszące świadomość i kulturę bezpieczeństwa w organizacji	ZCYB_I_U15	P6S_UO	3																		x						x														x								
Umie posługiwać się językiem obcym (na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego) w zakresie zarządzania i cyberbezpieczeństwa, w tym w środowisku pracy	ZCYB_I_U16	PRK6_UK	9																		x		x							x		x	x	x		x	x												x
Umie krytycznie oceniać i aktualizować własną wiedzę oraz doskonalić kompetencje zawodowe w obszarze cyberbezpieczeństwa	ZCYB_I_U17	PRK6_UU	7					x	x			x	x	x																						x	x												
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:				2	2	1	2	2	2	2	2	2	2	1	2	1	3	2	2	2	2	2	2	1	2	2	3	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Jest gotów do współpracy w zespołach oraz skutecznej komunikacji z różnymi grupami interesariuszy w środowisku zawodowym.	ZCYB_I_K01	PRK6_KR	16		x						x		x				x		x		x					x	x	x			x							x				x			x		x	x	x
Jest gotów do uwzględniania konsekwencji społecznych, prawnych i etycznych działań w zakresie zarządzania cyberbezpieczeństwem	ZCYB_I_K02	P6S_KO	16	x			x		x	x				x	x			x		x		x			x					x								x	x		x		x		x			
Jest gotów do przestrzegania zasad etyki zawodowej i promowania kultury bezpieczeństwa informacji	ZCYB_I_K03	PRK6_KO	11		x				x	x		x			x									x	x						x							x					x	x					
Jest gotów do krytycznej samooceny własnych kompetencji i planowania rozwoju zawodowego w obszarze zarządzania cyberbezpieczeństwem	ZCYB_I_K04	PRK6_KK	9					x			x								x									x							x	x	x							x				x
Jest gotów do korzystania z wiedzy ekspertów i współpracy specjalistycznej w celu rozwiązywania problemów poznawczych i praktycznych	ZCYB_I_K05	PRK6_KK	10	x		x		x								x				x			x						x						x										x	x		
Jest gotów do podejmowania inicjatyw i działań podnoszących poziom bezpieczeństwa informacji i kultury organizacyjnej, w sposób przedsiębiorczy i innowacyjny	ZCYB_I_K06	PRK6_KR	11										x				x	x								x	x			x									x	x	x		x					x	
Jest gotów do otwartego przyjmowania krytyki i dążenia do stałego rozwoju osobistego oraz zespołowego	ZCYB_I_K07	PRK6_KR	7				x					x										x										x	x	x		x													
Jest gotów do kształtowania proaktywnej postawy w dzieleniu się wiedzą i doświadczeniami	ZCYB_I_K08	PRK6_KO	9														x				x		x				x					x	x	x			x				x								

Macierz efektów uczenia się
Uczelnia: **Uniwersytet Dolnośląski DSW**
Wydział: **Studiów Stosowanych**
Kierunek: **Zarządzanie cyberbezpieczeństwem**
Moduł kształcenia wybieralnego / w zakresie ***Biały Wywiad w zarządzaniu cyberbezpieczeństwem***
Stopień kształcenia: **Licencjat (I stopień)**
Profil: **Praktyczny**
Czas trwania **6 semestrów**
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)							
				Wprowadzenie do cyberbezpieczeństwa	Podstawy zarządzania	Podstawy ekonomii	Psychologia cyberbezpieczeństwa	Logika i krytyczne myślenie	Etyka i prywatność danych	Aspekty prawne i regulacje w cyberbezpieczeństwie	Technologie informatyczne	Kompetencje przyszłości I	Kompetencje przyszłości II	Kompetencje przyszłości III	Szkolenie wstępne z zakresu BHP	Systemy ICT w cyberbezpieczeństwie	Cyfrowe zarządzanie projektami (Gantt, asana, kanban)	Zarządzanie ryzykiem w cyberprzestrzeni	Organizacja i zarządzanie	Cyberbezpieczeństwo operacyjne (wprow., narz.: SIEM i SOAR, SOC)	Warsztat pracy z grupą	Modelowanie cyberzagrożeń	Biały wywiad (OSINT) i analiza informacji	Testowanie i audyty cyberbezpieczeństwa	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	Analiza i zarządzanie podatnościami	Kultura bezpieczeństwa organizacji	Praktyki zarządzania incydentami	Podstawy Threat Intelligence	Socjologia dezinformacji i wojen informacyjnych	Role i uprawnienia w bezpieczeństwie informacji	Język obcy I (angielski, j.niemiecki)	Język obcy II (angielski, j.niemiecki)	Język obcy III (angielski, j.niemiecki)	Metodologia badań	Seminarium I	Seminarium II	Praktyka zawodowa ogólna I	Praktyka zawodowa ogólna II	Praktyka zawodowa kierunkowa I	Praktyka zawodowa kierunkowa II	Psychologia śledcza i profilowanie w cyberprzestrzeni	Psychologia poznawcza w wywiadzie i analizie danych	Zarządzanie stresem i efektywność pracy	Źródła danych dla białego wywiadu	OSINT i analiza behawioralna	Narzędzia i AI w służbie białego wywiadu	Analiza informacji i raportowanie	Design Thinking w cyberbezpieczeństwie
WIEDZA **absolwent zna i rozumie:**				**3**	**3**	**2**	**2**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**3**	**3**	**3**	**2**	**3**	**3**	**1**	**3**	**3**	**2**	**3**	**4**	**2**	**3**	**3**	**0**	**0**	**0**	**0**	**1**	**0**	**2**	**2**	**2**	**2**	**2**	**3**	**3**	**3**	**3**	**3**	**3**
W zaawansowanym stopniu zna i opisuje kluczowe koncepcje zarządzania i cyberbezpieczeństwa oraz ich powiązania z funkcjonowaniem organizacji	ZCYB_I_W01	PRK6_WG	**5**	x	x	x																															x							x	
W zaawansowanym stopniu zna funkcje zarządzania oraz rozumie ich zastosowanie w praktyce organizacji	ZCYB_I_W02	PRK6_WG	**10**		x	x											x	x	x	x								x									x				x				x
W zaawansowanym stopniu zna elementy architektury systemów ICT oraz narzędzia wspierające zapewnienie bezpieczeństwa organizacji	ZCYB_I_W03	PRK6_WG	**7**	x							x					x				x		x																					x		x	
W zaawansowanym stopniu zna i klasyfikuje rodzaje zagrożeń, podatności i incydentów w cyberprzestrzeni oraz ich wpływ na funkcjonowanie organizacji	ZCYB_I_W04	PRK6_WG	**11**	x														x			x				x		x	x	x									x					x			
W zaawansowanym stopniu zna i rozumie istotę strategii zarządzania bezpieczeństwem informacji, w tym procesy analizy ryzyka, audytu bezpieczeństwa oraz zarządzania ciągłością działania	ZCYB_I_W05	PRK6_WK	**7**															x	x					x	x				x							x									
W zaawansowanym stopniu zna modele organizacyjne oraz rozumie zasady funkcjonowania zespołów operacyjnych w kontekście bezpieczeństwa	ZCYB_I_W06	PRK6_WK	**3**		x																	x			x																				
W zaawansowanym stopniu zna normy, standardy i przepisy prawne wpływające na procesy zarządzania bezpieczeństwem informacji	ZCYB_I_W07	PRK6_WG	**7**						x	x					x									x	x				x									x							
W zaawansowanym stopniu zna psychologiczne i społeczne aspekty cyberzagrożeń	ZCYB_I_W08	PRK6_WG	**8**				x													x								x														x	x	x		x		
W zaawansowanym stopniu zna metody i techniki zarządzania projektami i procesami w obszarze bezpieczeństwa informacji	ZCYB_I_W09	PRK6_WG	**3**														x			x																					x					
W zaawansowanym stopniu zna i rozumie znaczenie zarządzania wiedzą i budowania kultury bezpieczeństwa w organizacji	ZCYB_I_W10	PRK6_WG	**3**																										x																x
W zaawansowanym stopniu zna techniki monitorowania i analizy zagrożeń (SIEM/SOAR, OSINT) oraz ich zastosowanie w praktyce organizacyjnej	ZCYB_I_W11	PRK6_WK	**8**								x					x				x			x						x													x	x	x			
W zaawansowanym stopniu zna zasady ochrony informacji, danych osobowych, prywatności oraz etyki w środowisku cyfrowym	ZCYB_I_W12	PRK6_WK	**6**							x					x									x					x														x			
W zaawansowanym stopniu zna metody projektowania scenariuszy reakcji na incydenty oraz planów ciągłości działania organizacji	ZCYB_I_W13	PRK6_WK	**4**																		x						x		x																x	
W zaawansowanym stopniu zna zasady rozwoju kompetencji zawodowych i uczenia się przez całe życie w obszarze zarządzania cyberbezpieczeństwem	ZCYB_I_W14	PRK6_WK	**6**									x	x	x																													x			x		
W zaawansowanym stopniu zna i rozumie znaczenie społecznej odpowiedzialności i konsekwencje działań związanych z cyberbezpieczeństwem	ZCYB_I_W15	PRK6_WK	**8**				x	x	x																				x														x			x		x
UMIEJĘTNOŚCI **absolwent potrafi:**				**1**	**1**	**0**	**1**	**3**	**3**	**2**	**2**	**3**	**3**	**3**	**2**	**2**	**3**	**3**	**3**	**3**	**4**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**2**	**1**	**1**	**1**	**0**	**3**	**3**	**2**	**2**	**2**	**2**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**3**
Umie analizować i oceniać problemy organizacyjne oraz zagrożenia cybernetyczne, proponując adekwatne rozwiązania zarządcze i techniczne	ZCYB_I_U01	PRK6_UW	**9**					x									x				x		x						x													x	x		x		x	
Umie prowadzić skuteczną komunikację oraz koordynować działania w sytuacjach kryzysowych	ZCYB_I_U02	PRK6_UK	**6**														x				x							x		x													x	x					
Umie wykorzystywać techniki OSINT i narzędzia analityczne w identyfikacji podatności i analizie ryzyka	ZCYB_I_U03	PRK6_UW	**12**	x							x					x				x			x			x			x													x	x		x	x	x	
Umie projektować i realizować działania rozwijające i wspierające kulturę bezpieczeństwa w organizacji	ZCYB_I_U04	PRK6_UO	**4**				x														x				x																						x
Umie przeprowadzać audyty i testy bezpieczeństwa oraz opracowywać stosowną dokumentację zgodnie z obowiązującymi standardami	ZCYB_I_U05	PRK6_UW	**5**					x		x													x	x																			x					
Umie stosować narzędzia do monitoringu oraz analizy cyberzagrożeń (SIEM, SOAR, OSINT) i oceniać efektywność zabezpieczeń	ZCYB_I_U06	PRK6_UW	**7**								x					x				x				x		x																	x	x				
Umie opracowywać, wdrażać i aktualizować procedury reagowania na incydenty bezpieczeństwa informacji	ZCYB_I_U07	PRK6_UW	**4**																	x						x		x																x				
Umie stosować strategie zarządzania zmianą i dostosowywać działania organizacyjne do dynamicznego otoczenia technologicznego.	ZCYB_I_U08	PRK6_UW	**4**														x	x											x															x				
Umie planować, organizować i kontrolować zadania zespołów oraz zarządzać projektami w obszarze bezpieczeństwa informacji	ZCYB_I_U09	PRK6_UO	**5**		x												x		x																								x					
Umie planować i realizować działania zapewniające ciągłość działania oraz organizować reakcje awaryjne	ZCYB_I_U10	PRK6_UW	**3**												x														x																		
Umie stosować przepisy prawne, normy branżowe i zasady etyki w praktyce zawodowej w zakresie zarządzania bezpieczeństwem	ZCYB_I_U11	P6S_UW	**6**						x	x					x								x						x																	
Umie efektywnie współpracować w zespołach interdyscyplinarnych oraz komunikować się z różnymi grupami interesariuszy	ZCYB_I_U12	PRK6_UK	**6**									x	x	x			x					x																									x

Umie przygotowywać raporty i prezentacje opisujące stany i incydenty bezpieczeństwa, rekomendując działania zaradcze	ZCYB_I_U13	PRK6_UK	**6**						x														x													x	x									x		x	
Umie efektywnie organizować pracę własną i zespołową, delegować zadania i działać pod presją czasu	ZCYB_I_U14	P6S_UO	**9**									x	x	x			x		x		x																	x						x					x
Umie planować i wdrażać działania podnoszące świadomość i kulturę bezpieczeństwa w organizacji	ZCYB_I_U15	P6S_UO	**3**																		x						x													x								
Umie posługiwać się językiem obcym (na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego) w zakresie zarządzania i cyberbezpieczeństwa, w tym w środowisku pracy	ZCYB_I_U16	PRK6_UK	**9**																		x		x							x		x	x	x		x	x											x	
Umie krytycznie oceniać i aktualizować własną wiedzę oraz doskonalić kompetencje zawodowe w obszarze cyberbezpieczeństwa	ZCYB_I_U17	PRK6_UU	**8**					x	x			x	x	x																						x	x						x						
KOMPETENCJE SPOŁECZNE absolwent jest gotów do:				**2**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**3**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
Jest gotów do współpracy w zespołach oraz skutecznej komunikacji z różnymi grupami interesariuszy w środowisku zawodowym.	ZCYB_I_K01	PRK6_KR	**12**		x						x		x				x		x		x					x	x	x			x							x										x	
Jest gotów do uwzględniania konsekwencji społecznych, prawnych i etycznych działań w zakresie zarządzania cyberbezpieczeństwem	ZCYB_I_K02	P6S_KO	**15**	x			x		x	x				x	x			x		x		x			x					x									x	x		x				x			
Jest gotów do przestrzegania zasad etyki zawodowej i promowania kultury bezpieczeństwa informacji	ZCYB_I_K03	PRK6_KO	**10**		x				x	x		x			x									x	x						x							x									x		
Jest gotów do krytycznej samooceny własnych kompetencji i planowania rozwoju zawodowego w obszarze zarządzania cyberbezpieczeństwem	ZCYB_I_K04	PRK6_KK	**10**					x			x								x									x							x	x	x						x	x				x	
Jest gotów do korzystania z wiedzy ekspertów i współpracy specjalistycznej w celu rozwiązywania problemów poznawczych i praktycznych	ZCYB_I_K05	PRK6_KK	**11**	x		x		x								x				x			x						x						x								x		x	x			
Jest gotów do podejmowania inicjatyw i działań podnoszących poziom bezpieczeństwa informacji i kultury organizacyjnej, w sposób przedsiębiorczy i innowacyjny	ZCYB_I_K06	PRK6_KR	**11**										x				x	x								x	x			x									x	x	x						x		x
Jest gotów do otwartego przyjmowania krytyki i dążenia do stałego rozwoju osobistego oraz zespołowego	ZCYB_I_K07	PRK6_KR	**8**				x					x										x										x	x	x		x						x							
Jest gotów do kształtowania proaktywnej postawy w dzieleniu się wiedzą i doświadczeniami	ZCYB_I_K08	PRK6_KO	**12**														x				x		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: ***Biały Wywiad w zarządzaniu cyberbezpieczeństwem***

Stopień kształcenia: **I stopień**

Profil: **praktyczny**

Forma studiów: **niestacjonarne**

Czas trwania: **3 lata (6 semestrów)**

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

			SUMA W %					39,94%	5,22%	54,94%	77%	32%	10%	96%	4%	60%	40%
			SUMA PUNKTÓW ECTS	180				71,9	9,4	98,9	137,7	58,0	18,2	172,0	8,0	108,2	71,8
					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 bepieczeństwie
Moduły kształcenia podstawowego																			
1	N1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		3,0	2,0
2	N1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		5,0	
3	N1-00-PODSTEKON-2	Podstawy ekonomii	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
4	N1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		4,0	1,0
5	N1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6		5,0	5,0	
6	N1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	14	0	14	0	0,6	0,0	2,4	3,0	0,0	0,0		3,0	3,0	
7	N1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		3,0	1,0
8	N1-00-TECHNINFO-1	Technologie informatyczne	O	3	14	0	14	0	0,6	0,0	2,4	3,0	0,0	0,0	3,0			3,0
9	N1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	0,0	0,0	2,0		2,0	
10	N1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
11	N1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
12	N1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,2	0,0			

Moduły kształcenia kierunkowego																			
1	N1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		2,0	3,0
2	N1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	28	0	18	10	0,7	0,4	2,9	4,0	0,0	0,4	4,0		4,0	
3	N1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		2,0	1,0
4	N1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
5	N1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		1,0	3,0
6	N1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	14	0	14	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0		2,0	
7	N1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	30	0	20	10	0,8	0,4	1,8	3,0	0,0	0,4	3,0			3,0
8	N1-00-OSINTANAL-2	Biały wywiad (OSINT) i analiza informacji	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0			5,0
9	N1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	34	12	12	10	1,0	0,4	2,6	2,6	0,0	0,9	4,0			4,0
10	N1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
11	N1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		2,0	1,0
12	N1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		3,0	0,0
13	N1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0			4,0
14	N1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	14	14	0	0	0,6	0,0	1,4	0,0	0,0	0,6	2,0			2,0
15	N1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	24	0	14	10	0,6	0,4	2,0	3,0	0,0	0,4	3,0		3,0	
16	N1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	14	0	14	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0			2,0
Moduły przygotowania pracy dyplomowej																			
1	N1-00-PROSEM-4	Metodologia badań	O	2	12	0	12	0	0,5	0,0	1,5	2,0	0,0	0,0	2,0		1,2	0,8
2	N1-00-SEMDYP1-5	Seminarium I	O	3	18	0	18	0	0,7	0,0	2,3	3,0	0,0	0,0	3,0		1,8	1,2
3	N1-00-SEMDYP2-6	Seminarium II	O	7	24	0	24	0	1,0	0,0	6,0	7,0	0,0	0,0	7,0		4,2	2,8
Moduły kształcenia językowego																			
1	N1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
2	N1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
3	N1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
Moduły kształcenia specjalnościowego																			
1	N1-00-PSYCHSLED-3	Psychologia śledcza i profilowanie w cyberprzestrzeni	O	3	18	0	18	0	0,7	0,0	2,3	3,0	3,0	0,0	3,0			3,0
2	N1-00-PSYCHPOZN-4	Psychologia poznawcza w wywiadzie i analizie	O	3	18	0	18	0	0,7	0,0	2,3	3,0	3,0	0,0	3,0			3,0
3	N1-00-PSYCHPOZAN-3	Zarządzanie stresem i efektywność pracy	O	3	18	0	18	0	0,7	0,0	2,3	3,0	3,0	0,0	3,0		3,0	
4	N1-00-ZRODANOS-3	Źródła danych dla białego wywiadu	O	2	14	14	0	0	0,6	0,0	1,4	0,0	2,0	0,6	2,0		2,0	
5	N1-00-OSINTBEH-4	OSINT i analiza behawioralna	O	3	20	0	20	0	0,8	0,0	2,2	3,0	3,0	0,0	3,0			3,0
6	N1-00-NARZAISLU-4	Narzędzia i AI w służbie białego wywiadu	O	3	20	0	20	0	0,8	0,0	2,2	3,0	3,0	0,0	3,0			3,0
7	N1-00-ANALINFOR-5	Analiza informacji i raportowanie	O	3	24	12	12	0	1,0	0,0	2,0	1,5	3,0	0,5	3,0		3,0	
8	N1-00-DSGTHCYB-6	Design Thinking w cyberbezpieczenieństwie	O	3	26	0	16	10	0,6	0,4	2,0	3,0	3,0	0,4	3,0		3,0	

Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	N1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0			13,0		7,8	5,2
2	N1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0			6,0		3,6	2,4
3	N1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0	13,0		13,0		7,8	5,2
4	N1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0	6,0		6,0		3,6	2,4

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Zarządzanie zespołami operacyjnymi IT***

Stopień kształcenia: **I stopień**

Profil: **praktyczny**

Forma studiów: **niestacjonarne**

Czas trwania: **3 lata (6 semestrów)**

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

			SUMA W %						40,00%	5,22%	54,89%	77%	32%	10%	96%	4%	60%	40%
			SUMA PUNKTÓW ECTS	180					72,0	9,4	98,8	138,3	58,0	18,2	172,0	8,0	108,2	71,8
					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 bepieczeństwie
Moduły kształcenia podstawowego																		
1	N1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		3,0	2,0
2	N1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		5,0	
3	N1-00-PODSTEKON-2	Podstawy ekonomii	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
4	N1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		4,0	1,0
5	N1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6		5,0	5,0	
6	N1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	14	0	14	0	0,6	0,0	2,4	3,0	0,0	0,0		3,0	3,0	
7	N1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		3,0	1,0
8	N1-00-TECHNINFO-1	Technologie informatyczne	O	3	14	0	14	0	0,6	0,0	2,4	3,0	0,0	0,0	3,0			3,0
9	N1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	0,0	0,0	2,0		2,0	
10	N1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
11	N1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
12	N1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,2	0,0			

Moduły kształcenia kierunkowego																			
1	N1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		2,0	3,0
2	N1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	28	0	18	10	0,7	0,4	2,9	4,0	0,0	0,4	4,0		4,0	
3	N1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		2,0	1,0
4	N1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
5	N1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		1,0	3,0
6	N1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	14	0	14	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0		2,0	
7	N1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	30	0	20	10	0,8	0,4	1,8	3,0	0,0	0,4	3,0			3,0
8	N1-00-OSINTANAL-2	Biały wywiad (OSINT) i analiza informacji	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0			5,0
9	N1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	34	12	12	10	1,0	0,4	2,6	2,6	0,0	0,9	4,0			4,0
10	N1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
11	N1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		2,0	1,0
12	N1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		3,0	0,0
13	N1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0			4,0
14	N1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	14	14	0	0	0,6	0,0	1,4	0,0	0,0	0,6	2,0			2,0
15	N1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	24	0	14	10	0,6	0,4	2,0	3,0	0,0	0,4	3,0		3,0	
16	N1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	14	0	14	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0			2,0
Moduły przygotowania pracy dyplomowej																			
1	N1-00-PROSEM-4	Metodologia badań	O	2	12	0	12	0	0,5	0,0	1,5	2,0	0,0	0,0	2,0		1,2	0,8
2	N1-00-SEMDYP1-5	Seminarium I	O	3	18	0	18	0	0,7	0,0	2,3	3,0	0,0	0,0	3,0		1,8	1,2
3	N1-00-SEMDYP2-6	Seminarium II	O	7	24	0	24	0	1,0	0,0	6,0	7,0	0,0	0,0	7,0		4,2	2,8
Moduły kształcenia językowego																			
1	N1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
2	N1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
3	N1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
Moduły kształcenia specjalnościowego																			
1	N1-00-BEZFIZINF-3	Bezpieczeństwo fizyczne, środowiskowe i infrastruktury	O	3	30	14	16	0	1,2	0,0	1,8	1,6	3,0	0,6	3,0			3,0
2	N1-00-AUDINCODP-4	Audyt incydentów i odporności	O	3	18	0	18	0	0,7	0,0	2,3	3,0	3,0	0,0	3,0			3,0
3	N1-00-TESTPENME-3	Testy penetracyjne i metody ofensywne	O	3	20	0	20	0	0,8	0,0	2,2	3,0	3,0	0,0	3,0			3,0
4	N1-00-WSPSOCZESP-4	Współpraca SOC i zespołów ds. ryzyka	O	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
5	N1-00-NARZMONIT-4	Narzędzia monitoringu i automatyzacji (SIEM i SOAR)	O	3	24	12	12	0	1,0	0,0	2,0	1,5	3,0	0,5	3,0			3,0
6	N1-00-ANALSTROP-4	Analiza strat i utrzymanie ciągłości operacyjnej	O	3	12	0	12	0	0,5	0,0	2,5	3,0	3,0	0,0	3,0		3,0	
7	N1-00-TWSCENINC-5	Tworzenie scenariuszy reakcji na incydenty	O	3	22	0	12	10	0,5	0,4	2,1	3,0	3,0	0,4	3,0		3,0	
8	N1-00-ZARZSTRATK-6	Zarządzanie stresem w trakcie ataku	O	3	20	0	20	0	0,8	0,0	2,2	3,0	3,0	0,0	3,0		3,0	

Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	N1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0			13,0		7,8	5,2
2	N1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0			6,0		3,6	2,4
3	N1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0	13,0		13,0		7,8	5,2
4	N1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0	6,0		6,0		3,6	2,4

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Cyberhigiena i edukacja informacyjna***

Stopień kształcenia: **I stopień**

Profil: **praktyczny**

Forma studiów: **niestacjonarne**

Czas trwania: **3 lata (6 semestrów)**

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

			SUMA W %						40,00%	5,22%	54,89%	77%	32%	10%	96%	4%	60%	40%
			SUMA PUNKTÓW ECTS	180					72,0	9,4	98,8	138,3	58,0	18,2	172,0	8,0	108,2	71,8
					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 bepieczeństwie
Moduły kształcenia podstawowego																		
1	N1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		3,0	2,0
2	N1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		5,0	
3	N1-00-PODSTEKON-2	Podstawy ekonomii	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
4	N1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		4,0	1,0
5	N1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6		5,0	5,0	
6	N1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	14	0	14	0	0,6	0,0	2,4	3,0	0,0	0,0		3,0	3,0	
7	N1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		3,0	1,0
8	N1-00-TECHNINFO-1	Technologie informatyczne	O	3	14	0	14	0	0,6	0,0	2,4	3,0	0,0	0,0	3,0			3,0
9	N1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	0,0	0,0	2,0		2,0	
10	N1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
11	N1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
12	N1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,2	0,0			

Moduły kształcenia kierunkowego																			
1	N1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0		2,0	3,0
2	N1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	28	0	18	10	0,7	0,4	2,9	4,0	0,0	0,4	4,0		4,0	
3	N1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		2,0	1,0
4	N1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
5	N1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		1,0	3,0
6	N1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	14	0	14	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0		2,0	
7	N1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	30	0	20	10	0,8	0,4	1,8	3,0	0,0	0,4	3,0			3,0
8	N1-00-OSINTANAL-2	Biały wywiad (OSINT) i analiza informacji	E	5	32	14	18	0	1,3	0,0	3,7	2,8	0,0	0,6	5,0			5,0
9	N1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	34	12	12	10	1,0	0,4	2,6	2,6	0,0	0,9	4,0			4,0
10	N1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0		4,0	
11	N1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		2,0	1,0
12	N1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	20	0	20	0	0,8	0,0	2,2	3,0	0,0	0,0	3,0		3,0	0,0
13	N1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	28	12	16	0	1,1	0,0	2,9	2,3	0,0	0,5	4,0			4,0
14	N1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	14	14	0	0	0,6	0,0	1,4	0,0	0,0	0,6	2,0			2,0
15	N1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	24	0	14	10	0,6	0,4	2,0	3,0	0,0	0,4	3,0		3,0	
16	N1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	14	0	14	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0			2,0
Moduły przygotowania pracy dyplomowej																			
1	N1-00-PROSEM-4	Metodologia badań	O	2	12	0	12	0	0,5	0,0	1,5	2,0	0,0	0,0	2,0		1,2	0,8
2	N1-00-SEMDYP1-5	Seminarium I	O	3	18	0	18	0	0,7	0,0	2,3	3,0	0,0	0,0	3,0		1,8	1,2
3	N1-00-SEMDYP2-6	Seminarium II	O	7	24	0	24	0	1,0	0,0	6,0	7,0	0,0	0,0	7,0		4,2	2,8
Moduły kształcenia językowego																			
1	N1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
2	N1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
3	N1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	76	0	16	60	0,6	2,4	1,0	0,0	4,0	2,4	4,0		2,4	1,6
Moduły kształcenia specjalnościowego																			
1	N1-00-CYBERGRSP-3	Cyberbezpieczeństwo wybranych grup społecznych - modele zarządzania ryzykiem	O	3	30	14	16	0	1,2	0,0	1,8	1,6	3,0	0,6	3,0			3,0
2	N1-00-STRZARRLUD-4	Strategie zarządzania ryzykiem ludzkim w	O	3	18	0	18	0	0,7	0,0	2,3	3,0	3,0	0,0	3,0		3,0	
3	N1-00-BEZUZALTE-3	Bezpieczeństwo organizacji wobec uzależnień technologicznych	O	3	20	0	20	0	0,8	0,0	2,2	3,0	3,0	0,0	3,0			3,0
4	N1-00-TECHEDU-4	Technologie wspierające edukację i monitorowanie efektywności	O	2	12	0	12	0	0,5	0,0	1,5	2,0	2,0	0,0	2,0		2,0	
5	N1-00-PROJNARE-4	Projektowanie i zarządzanie narzędziami edukacyjnymi	O	3	24	12	12	0	1,0	0,0	2,0	1,5	3,0	0,5	3,0			3,0
6	N1-00-PROJELEARN-4	Projektowanie interaktywnych szkoleń i e-learningu - aspekty wdrożeniowe	O	3	12	0	12	0	0,5	0,0	2,5	3,0	3,0	0,0	3,0			3,0

7	N1-00-WDZPSYCH-5	Wspieranie zdrowia psychicznego pracowników w środowisku cyfrowym	O	3	22	0	12	10	0,5	0,4	2,1	3,0	3,0	0,4	3,0		3,0	
8	N1-00-METODEFEK-6	Metody badania efektywności programów edukacyjnych bezpieczeństwa i zarządzania jakością edukacji	O	3	20	0	20	0	0,8	0,0	2,2	3,0	3,0	0,0	3,0		3,0	
Moduły praktyk specjalnościowych(wybieralnych)																		
					ogół.	WP	EW	prak.										
1	N1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0			13,0		7,8	5,2
2	N1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0			6,0		3,6	2,4
3	N1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0	13,0		13,0		7,8	5,2
4	N1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0	6,0		6,0		3,6	2,4

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Biały wywiad w zarządzaniu cyberbezpieczeństwem***

Stopień kształcenia: **I stopień**

Profil: **praktyczny**

Forma studiów: **stacjonarne**

Czas trwania: **3 lata (6 semestrów)**

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

			SUMA W %						53,89%	5,61%	40,61%	74%	32%	15%	96%	4%	60%	40%
			SUMA PUNKTÓW ECTS	180					97,0	10,1	73,1	132,5	58,0	27,3	172,0	8,0	108,2	71,8
					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 bepieczeństwie
Moduły kształcenia podstawowego																		
1	S1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		3,0	2,0
2	S1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		5,0	
3	S1-00-PODSTEKON-2	Podstawy ekonomii	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
4	S1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		4,0	1,0
5	S1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2		5,0	5,0	
6	S1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0		3,0	3,0	
7	S1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		3,0	1,0
8	S1-00-TECHNINFO-1	Technologie informatyczne	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0			3,0
9	S1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0		2,0	
10	S1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	2,0	0,0	2,0		2,0	
11	S1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	2,0	0,0	2,0		2,0	
12	S1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,2	0,0			

Moduły kształcenia kierunkowego																			
1	S1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		2,0	3,0
2	S1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	50	0	30	20	1,2	0,8	2,0	4,0	0,0	0,8	4,0		4,0	
3	S1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	0,0	3,0		2,0	1,0
4	S1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
5	S1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		1,0	3,0
6	S1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	26	0	26	0	1,0	0,0	1,0	2,0	0,0	0,0	2,0		2,0	
7	S1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	54	0	36	18	1,4	0,7	0,9	3,0	0,0	0,7	3,0			3,0
8	S1-00-OSINTANAL-2	Biały wywiad (OSINT) i analiza informacji	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0			5,0
9	S1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	50	20	20	10	1,6	0,4	2,0	2,4	0,0	1,2	4,0			4,0
10	S1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
11	S1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		2,0	1,0
12	S1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		3,0	0,0
13	S1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	0,8	4,0			4,0
14	S1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	20	20	0	0	0,8	0,0	1,2	0,0	0,0	0,8	2,0			2,0
15	S1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	30	0	20	10	0,8	0,4	1,8	3,0	0,0	0,4	3,0		3,0	
16	S1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	20	0	20	0	0,8	0,0	1,2	2,0	0,0	0,0	2,0			2,0
Moduły przygotowania pracy dyplomowej																			
1	S1-00-PROSEM-4	Metodologia badań	O	2	20	0	20	0	0,8	0,0	1,2	2,0	0,0	0,0	2,0		1,2	0,8
2	S1-00-SEMDYP1-5	Seminarium I	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		1,8	1,2
3	S1-00-SEMDYP2-6	Seminarium II	O	7	40	0	40	0	1,6	0,0	5,4	7,0	0,0	0,0	7,0		4,2	2,8
Moduły kształcenia językowego																			
1	S1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
2	S1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
3	S1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
Moduły kształcenia specjalnościowego																			
1	S1-00-PSYCHSLED-3	Psychologia śledcza i profilowanie w cyberprzestrzeni	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
2	S1-00-PSYCHPOZN-4	Psychologia poznawcza w wywiadzie i analizie	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
3	S1-00-PSYCHPOZAN-3	Zarządzanie stresem i efektywność pracy	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0		3,0	
4	S1-00-ZRODANOS-3	Źródła danych dla białego wywiadu	O	2	20	20	0	0	0,8	0,0	1,2	0,0	2,0	0,8	2,0		2,0	
5	S1-00-OSINTBEH-4	OSINT i analiza behawioralna	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
6	S1-00-NARZAISLU-4	Narzędzia i AI w służbie białego wywiadu	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
7	S1-00-ANALINFOR-5	Analiza informacji i raportowanie	O	3	44	20	24	0	1,8	0,0	1,2	1,7	3,0	0,8	3,0		3,0	
8	S1-00-DSGTHCYB-6	Design Thinking w cyberbezpieczenieństwie	O	3	40	0	30	10	1,2	0,4	1,4	3,0	3,0	0,4	3,0		3,0	

Moduły praktyk specjalnościowych(wybieralnych)																		
1	S1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0			13,0		7,8	5,2
2	S1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0			6,0		3,6	2,4
3	S1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0	13,0		13,0		7,8	5,2
4	S1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0	6,0		6,0		3,6	2,4

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Zarządzanie zespołami operacyjnymi IT***

Stopień kształcenia: **I stopień**

Profil: **praktyczny**

Forma studiów: **stacjonarne**

Czas trwania: **3 lata (6 semestrów)**

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

			SUMA W %					53,89%	5,61%	40,61%	74%	32%	15%	96%	4%	60%	40%
			SUMA PUNKTÓW ECTS	180				97,0	10,1	73,1	132,8	58,0	27,3	172,0	8,0	108,2	71,8
					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 bepieczeństwie
Moduły kształcenia podstawowego																			
1	S1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		3,0	2,0
2	S1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		5,0	
3	S1-00-PODSTEKON-2	Podstawy ekonomii	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
4	S1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		4,0	1,0
5	S1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2		5,0	5,0	
6	S1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0		3,0	3,0	
7	S1-00-ASPPRAWCY-2	cyberbezpieczeństwie	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		3,0	1,0
8	S1-00-TECHNINFO-1	Technologie informatyczne	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0			3,0
9	S1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0		2,0	
10	S1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	2,0	0,0	2,0		2,0	
11	S1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	2,0	0,0	2,0		2,0	
12	S1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,2	0,0			

Moduły kształcenia kierunkowego																		
1	S1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		2,0	3,0
2	S1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	50	0	30	20	1,2	0,8	2,0	4,0	0,0	0,8	4,0		4,0	
3	S1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	0,0	3,0		2,0	1,0
4	S1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
5	S1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		1,0	3,0
6	S1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	26	0	26	0	1,0	0,0	1,0	2,0	0,0	0,0	2,0		2,0	
7	S1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	54	0	36	18	1,4	0,7	0,9	3,0	0,0	0,7	3,0			3,0
8	S1-00-OSINTANAL-2	Biały wywiad (OSINT) i analiza informacji	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0			5,0
9	S1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	50	20	20	10	1,6	0,4	2,0	2,4	0,0	1,2	4,0			4,0
10	S1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
11	S1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		2,0	1,0
12	S1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		3,0	0,0
13	S1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	0,8	4,0			4,0
14	S1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	20	20	0	0	0,8	0,0	1,2	0,0	0,0	0,8	2,0			2,0
15	S1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	30	0	20	10	0,8	0,4	1,8	3,0	0,0	0,4	3,0		3,0	
16	S1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	20	0	20	0	0,8	0,0	1,2	2,0	0,0	0,0	2,0			2,0
Moduły przygotowania pracy dyplomowej																		
1	S1-00-PROSEM-4	Metodologia badań	O	2	20	0	20	0	0,8	0,0	1,2	2,0	0,0	0,0	2,0		1,2	0,8
2	S1-00-SEMDYP1-5	Seminarium I	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		1,8	1,2
3	S1-00-SEMDYP2-6	Seminarium II	O	7	40	0	40	0	1,6	0,0	5,4	7,0	0,0	0,0	7,0		4,2	2,8
Moduły kształcenia językowego																		
1	S1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
2	S1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
3	S1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6

Moduły kształcenia specjalnościowego																		
1	S1-00-BEZFIZINF-3	Bezpieczeństwo fizyczne, środowiskowe i infrastruktury	O	3	40	20	20	0	1,6	0,0	1,4	1,5	3,0	0,8	3,0			3,0
2	S1-00-AUDINCODP-4	Audyt incydentów i odporności	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
3	S1-00-TESTPENME-3	Testy penetracyjne i metody ofensywne	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
4	S1-00-WSPSOCZESP-4	Współpraca SOC i zespołów ds. ryzyka	O	2	20	0	20	0	0,8	0,0	1,2	2,0	2,0	0,0	2,0		2,0	
5	S1-00-NARZMONIT-4	Narzędzia monitoringu i automatyzacji (SIEM i SOAR)	O	3	40	20	20	0	1,6	0,0	1,4	1,5	3,0	0,8	3,0			3,0
6	S1-00-ANALSTROP-4	Analiza strat i utrzymanie ciągłości operacyjnej	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0		3,0	
7	S1-00-TWSCENINC-5	Tworzenie scenariuszy reakcji na incydenty	O	3	40	0	30	10	1,2	0,4	1,4	3,0	3,0	0,4	3,0		3,0	
8	S1-00-ZARZSTRATK-6	Zarządzanie stresem w trakcie ataku	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0		3,0	
Moduły praktyk specjalnościowych(wybieralnych)																		
1	S1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0			13,0		7,8	5,2
2	S1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0			6,0		3,6	2,4
3	S1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0	13,0		13,0		7,8	5,2
4	S1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0	6,0		6,0		3,6	2,4

Sumaryczne wskaźniki ECTS

Wydział: **Studiów Stosowanych we Wrocławiu**

Kierunek: **Zarządzanie cyberbezpieczeństwem**

Moduł kształcenia wybieralnego / w zakresie: ***Cyberhigiena i edukacja informacyjna***

Stopień kształcenia: **I stopień**

Profil: **praktyczny**

Forma studiów: **stacjonarne**

Czas trwania: **3 lata (6 semestrów)**

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

			SUMA W %					53,89%	5,61%	40,61%	74%	32%	15%	96%	4%	60%	40%
			SUMA PUNKTÓW ECTS	180				97,0	10,1	73,1	132,8	58,0	27,3	172,0	8,0	108,2	71,8
Lp.	Kod przedmiotu	Nazwa przedmiotu/modułu kształcenia	E/O/ZAL	ECTS	Liczba godz.				Wskaźniki 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 bepieczeństwie
Moduły kształcenia podstawowego																			
1	S1-00-WPRODCYBER-1	Wprowadzenie do cyberbezpieczeństwa	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		3,0	2,0
2	S1-00-PODSTZARZ-1	Podstawy zarządzania	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		5,0	
3	S1-00-PODSTEKON-2	Podstawy ekonomii	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
4	S1-00-PSYCHCYBER-2	Psychologia cyberbezpieczeństwa	O	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		4,0	1,0
5	S1-00-LOGKRYTMY-1	Logika i krytyczne myślenie	O	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2		5,0	5,0	
6	S1-00-ETYKPRYWD-2	Etyka i prywatność danych	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0		3,0	3,0	
7	S1-00-ASPPRAWCY-2	Aspekty prawne i regulacje w cyberbezpieczeństwie	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		3,0	1,0
8	S1-00-TECHNINFO-1	Technologie informatyczne	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0			3,0
9	S1-00-KOMPRZY1-1	Kompetencje przyszłości I	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	0,0	0,0	2,0		2,0	
10	S1-00-KOMPRZY2-2	Kompetencje przyszłości II	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	2,0	0,0	2,0		2,0	
11	S1-00-KOMPRZY3-3	Kompetencje przyszłości III	ZAL	2	16	0	16	0	0,6	0,0	1,4	2,0	2,0	0,0	2,0		2,0	
12	S1-00-BHP-1	Szkolenie wstępne z zakresu BHP	ZAL	0	4	0	0	4	0,0	0,2	0,0	0,0	0,0	0,2	0,0			

Moduły kształcenia kierunkowego																			
1	S1-00-SYSTICTCY-1	Systemy ICT w cyberbezpieczeństwie	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0		2,0	3,0
2	S1-00-CYFZARZPR-2	Cyfrowe zarządzanie projektami	O	4	50	0	30	20	1,2	0,8	2,0	4,0	0,0	0,8	4,0		4,0	
3	S1-00-ZARZRYZCY-6	Zarządzanie ryzykiem w cyberprzestrzeni	O	3	36	0	36	0	1,4	0,0	1,6	3,0	0,0	0,0	3,0		2,0	1,0
4	S1-00-ORGZARZAD-2	Organizacja i zarządzanie	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
5	S1-00-CYBOPERAC-2	Cyberbezpieczeństwo operacyjne (SIEM i SOAR, SOC)	O	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		1,0	3,0
6	S1-00-WARSZGRUP-6	Warsztat pracy z grupą	O	2	26	0	26	0	1,0	0,0	1,0	2,0	0,0	0,0	2,0		2,0	
7	S1-00-MODCYBEZA-5	Modelowanie cyberzagrożeń	O	3	54	0	36	18	1,4	0,7	0,9	3,0	0,0	0,7	3,0			3,0
8	S1-00-OSINTANAL-2	Biały wywiad (OSINT) i analiza informacji	E	5	60	30	30	0	2,4	0,0	2,6	2,5	0,0	1,2	5,0			5,0
9	S1-00-TESTAUDYC-6	Testowanie i audyty cyberbezpieczeństwa	O	4	50	20	20	10	1,6	0,4	2,0	2,4	0,0	1,2	4,0			4,0
10	S1-00-NORMJAKBE-4	Normy jakości i bezpieczeństwa informacji (ISO 27001, 9001)	E	4	50	30	20	0	2,0	0,0	2,0	1,6	0,0	1,2	4,0		4,0	
11	S1-00-ANALZARPO-4	Analiza i zarządzanie podatnościami	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		2,0	1,0
12	S1-00-KULTBEZOR-5	Kultura bezpieczeństwa organizacji	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		3,0	0,0
13	S1-00-PRAKZARZIN-6	Praktyki zarządzania incydentami	O	4	50	20	30	0	2,0	0,0	2,0	2,4	0,0	0,8	4,0			4,0
14	S1-00-PODTHINT-3	Podstawy Threat Intelligence	O	2	20	20	0	0	0,8	0,0	1,2	0,0	0,0	0,8	2,0			2,0
15	S1-00-SOCJDEZIN-4	Socjologia dezinformacji i wojen informacyjnych	O	3	30	0	20	10	0,8	0,4	1,8	3,0	0,0	0,4	3,0		3,0	
16	S1-00-ROLEUPBEZ-5	Role i uprawnienia w bezpieczeństwie informacji	O	2	20	0	20	0	0,8	0,0	1,2	2,0	0,0	0,0	2,0			2,0
Moduły przygotowania pracy dyplomowej																			
1	S1-00-PROSEM-4	Metodologia badań	O	2	20	0	20	0	0,8	0,0	1,2	2,0	0,0	0,0	2,0		1,2	0,8
2	S1-00-SEMDYP1-5	Seminarium I	O	3	30	0	30	0	1,2	0,0	1,8	3,0	0,0	0,0	3,0		1,8	1,2
3	S1-00-SEMDYP2-6	Seminarium II	O	7	40	0	40	0	1,6	0,0	5,4	7,0	0,0	0,0	7,0		4,2	2,8
Moduły kształcenia językowego																			
1	S1-00-JĘZOBC1-3	Język obcy I (język angielski, język niemiecki)	O	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
2	S1-00-JĘZOBC2-4	Język obcy II (język angielski, język niemiecki)	O	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
3	S1-00-JĘZOBC3-5	Język obcy III (język angielski, język niemiecki)	E	4	84	0	24	60	1,0	2,4	0,6	0,0	4,0	2,4	4,0		2,4	1,6
Moduły kształcenia specjalnościowego																			
1	S1-00-CYBERGRSP-3	Cyberbezpieczeństwo wybranych grup społecznych - modele zarządzania ryzykiem	O	3	40	20	20	0	1,6	0,0	1,4	1,5	3,0	0,8	3,0			3,0
2	S1-00-STRZARRLUD-4	Strategie zarządzania ryzykiem ludzkim w	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0		3,0	
3	S1-00-BEZUZALTE-3	Bezpieczeństwo organizacji wobec uzależnień technologicznych	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
4	S1-00-TECHEDU-4	Technologie wspierające edukację i monitorowanie efektywności	O	2	20	0	20	0	0,8	0,0	1,2	2,0	2,0	0,0	2,0		2,0	
5	S1-00-PROJNARE-4	Projektowanie i zarządzanie narzędziami edukacyjnymi	O	3	40	20	20	0	1,6	0,0	1,4	1,5	3,0	0,8	3,0			3,0
6	S1-00-PROJELEARN-4	Projektowanie interaktywnych szkoleń i e-learningu - aspekty wdrożeniowe	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0			3,0
7	S1-00-WDZPSYCH-5	Wspieranie zdrowia psychicznego pracowników w środowisku cyfrowym	O	3	40	0	30	10	1,2	0,4	1,4	3,0	3,0	0,4	3,0		3,0	

8	S1-00-METODEFEK-6	Metody badania efektywności programów edukacyjnych bezpieczeństwa i zarządzania jakością edukacji	O	3	36	0	36	0	1,4	0,0	1,6	3,0	3,0	0,0	3,0		3,0	
Moduły praktyk specjalnościowych(wybieralnych)																		
1	S1-00-PRAKZAWOG1-3	Praktyka zawodowa ogólna I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0			13,0		7,8	5,2
2	S1-00-PRAKZAWOG2-4	Praktyka zawodowa ogólna II	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0			6,0		3,6	2,4
3	S1-00-PRAKZAWKIE1-5	Praktyka zawodowa kierunkowa I	ZAL	13	320	2	10	308	12,8	0,0	0,2	13,0	13,0		13,0		7,8	5,2
4	S1-00-PRAKZAWSP1-6	Praktyka zawodowa specjalnościowa I	ZAL	6	160	2	10	148	6,0	0,0	0,0	6,0	6,0		6,0		3,6	2,4