Załącznik nr 2a do Uchwały Senatu UKEN nr ..... z dnia ..... 2026 r.

PROGRAM STUDIÓW WYŻSZYCH ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM 2026/2027

SPIS TREŚCI

OGÓLNA CHARAKTERYSTYKA KIERUNKU STUDIÓW 1
ZWIĄZEK Z MISJĄ UCZELNI I STRATEGIĄ JEJ ROZWOJU 2
WARUNKI REKRUTACJI 2
SYLWETKA ABSOLWENTA 3
UZYSKIWANE KWALIFIKACJE ORAZ UPRAWNIENIA ZAWODOWE 3
PRAKTYKI ZAWODOWE 4
OPIS ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ 4
EFEKTY UCZENIA SIĘ 5
MATRYCA ODNIESIEŃ EFEKTÓW WIEDZY DO UMIEJĘTNOŚCI 7
MATRYCA POKRYCIA EFEKTÓW KIERUNKOWYCH 8
SPOSOBY WERYFIKACJI I OCENY EFEKTÓW UCZENIA SIĘ 9
TREŚCI PROGRAMOWE ORAZ EFEKTY KIERUNKOWE 10
PLAN STUDIÓW – ZAŁĄCZNIK 3b 16

OGÓLNA CHARAKTERYSTYKA KIERUNKU STUDIÓW

Jednostka badawczo-dydaktyczna prowadząca kierunek:	INSTYTUT BEZPIECZEŃSTWA I INFORMATYKI
Nazwa kierunku:	CYBERBEZPIECZEŃSTWO
Poziom:	STUDIA II STOPNIA
Profil:	PRAKTYCZNY
Forma:	NIESTACJONARNE
Liczba punktów ECTS wymaganych do ukończenia studiów:	90 ECTS
Tytuł zawodowy nadawany absolwentom:	MAGISTER INŻYNIER
Poziom Polskiej Ramy Kwalifikacji:	SIÓDMY (7)
Termin rozpoczęcia cyklu:	2026/2027, SEMESTR LETNI
Czas trwania studiów (liczba semestrów):	3 SEMESTRY
Dziedzina/-y:	NAUKI INŻYNIERYJNO-TECHNICZNE
Dyscyplina:	INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA 100%
Kod ISCED:	0612 - PROJEKTOWANIE I ADMINISTROWANIE BAZ DANYCH I SIECI

PODSTAWOWE INFORMACJE O PROGRAMIE KSZTAŁCENIA I KIERUNKU STUDIÓW	CYBEZBEZPIECZEŃSTWO
Liczba semestrów	3
Łączna liczba godzin pracy studenta w planie studiów	600
Łączna liczba punktów ECTS konieczna do ukończenia studiów	90
Łączna liczba godzin przeznaczonych na praktyki zawodowe	480
Łączna liczba punktów ECTS przeznaczonych na praktyki zawodowe	14
Łączna liczba punktów ECTS przeznaczonych na pracę dyplomową	8
Procentowy udział w ramach zajęć w bezpośrednim udziale NA	34,9%
Łączna liczba punktów ECTS powiązanych z działalnością naukową	75
Łączna liczba punktów ECTS powiązanych z działalnością naukową w dyscyplinie ITiT	70
Łączna liczba punktów ECTS kształtujących umiejętności praktyczne	64,5
Łączna liczba punktów ECTS przyporządkowanych kursom z zakresu nauk human.-społ. (F)	5
Łączna liczba godzin zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	205
Łączna liczba punktów ECTS przyporządkowanych kursom do wyboru	27
Łączna liczba punktów ECTS - procentowy udział kursów do wyboru	30,0%
Łączna liczba godzin zajęć z języków obcych	15
Łączna liczba punktów ECTS przypisana zajęciom z języków obcych	1

ZWIĄZEK Z MISJĄ UCZELNI I STRATEGIĄ JEJ ROZWOJU

Kierunek Cyberbezpieczeństwo, studia drugiego stopnia o profilu praktycznym, jest w pełni zgodny z misją oraz Strategią Rozwoju Uniwersytetu Komisji Edukacji Narodowej w Krakowie na lata 2023–2030 i stanowi element realizacji jej kluczowych założeń. Zgodnie z misją Uczelni, zakładającą kształcenie nowoczesnych kadr dla gospodarki opartej na wiedzy oraz aktywne współdziałanie z otoczeniem społeczno-gospodarczym, program studiów na kierunku Cyberbezpieczeństwo ukierunkowany jest na przygotowanie wysoko wykwalifikowanych specjalistów posiadających pogłębione kompetencje praktyczne, analityczne i projektowe, odpowiadające aktualnym i przyszłym potrzebom rynku pracy. Kierunek wpisuje się w realizację Obszaru I - Kształcenie, w szczególności celu strategicznego „Doskonałość kształcenia", poprzez zapewnienie wysokiej jakości procesu dydaktycznego, systematyczne doskonalenie programów studiów, dostosowanie efektów uczenia się do potrzeb społeczno-gospodarczych oraz rozwój współpracy z interesariuszami zewnętrznymi. Realizowane są w tym zakresie m.in. cele operacyjne dotyczące podnoszenia jakości kształcenia, zwiększania konkurencyjności absolwentów oraz rozwijania oferty dydaktycznej, w tym na poziomie studiów drugiego stopnia. Jednocześnie kierunek realizuje założenia Obszaru II - Badania naukowe i rozwój dyscyplin, poprzez rozwijanie zaawansowanych kompetencji badawczych studentów, włączanie ich w realizację projektów naukowych oraz kształtowanie umiejętności analizy zagrożeń cybernetycznych, projektowania mechanizmów ochrony informacji oraz rozwiązywania złożonych problemów związanych z bezpieczeństwem systemów teleinformatycznych. Związek kierunku ze Strategią widoczny jest również w realizacji Obszaru III - Społeczna odpowiedzialność nauki, poprzez kształtowanie postaw etycznych, odpowiedzialności zawodowej oraz przygotowanie absolwentów do aktywnego uczestnictwa w rozwoju społeczeństwa informacyjnego i gospodarki cyfrowej, ze szczególnym uwzględnieniem ochrony danych, bezpieczeństwa informacji oraz odporności systemów cyfrowych na współczesne zagrożenia. Profil praktyczny studiów stanowi odpowiedź na wyzwania związane z dynamicznym rozwojem technologii cyfrowych, wzrostem liczby cyberzagrożeń oraz rosnącym znaczeniem bezpieczeństwa systemów informatycznych i infrastruktury krytycznej. Kierunek pozostaje w bezpośrednim związku z celami strategicznymi dotyczącymi dostosowania oferty dydaktycznej do potrzeb rynku pracy, wzmacniania kompetencji cyfrowych oraz zwiększania konkurencyjności absolwentów na rynku pracy.

WARUNKI REKRUTACJI

Studia przewidziane dla absolwentów studiów I stopnia z dyplomem inżyniera kierunku cyberbezpieczeństwo lub pokrewnych. Kwalifikacja kandydatów odbywa się na podstawie wyniku pisemnego egzaminu wstępnego. Zakres egzaminu wstępnego obejmuje zagadnienia z obszaru wiedzy i umiejętności właściwych dla absolwenta studiów pierwszego stopnia (inżynierskich) na kierunku Cyberbezpieczeństwo.

Egzamin pisemny wstępny złożony jest z pytań zamkniętych, 60 pytań jednokrotnego wyboru, punktowanie 1, maksymalna liczba punktów 60, czas trwania 60 minut. Wyniki egzaminu wyrażane są w punktach. Próg punktowy przyjęcia: 20 pkt.
O przyjęciu decyduje miejsce na liście rankingowej sporządzonej według liczby uzyskanych punktów, w ramach ustalonego limitu miejsc. W przypadku uzyskania przez kandydatów takiej samej liczby punktów, o kolejności na liście rankingowej decydują dodatkowe kryteria: średnia z całego toku studiów.

SYLWETKA ABSOLWENTA

Absolwent kierunku Cyberbezpieczeństwo, studiów drugiego stopnia o profilu praktycznym, posiada pogłębioną wiedzę z zakresu nowoczesnych rozwiązań informatycznych, bezpieczeństwa systemów teleinformatycznych oraz ochrony informacji w środowisku cyfrowym. Jest przygotowany do analizowania, projektowania i rozwijania rozwiązań służących zapewnieniu bezpieczeństwa infrastruktury IT, systemów sieciowych, aplikacji oraz danych przetwarzanych w organizacjach o różnym profilu działalności. Absolwent potrafi identyfikować i analizować zagrożenia cybernetyczne, oceniać ryzyko związane z funkcjonowaniem systemów informatycznych oraz dobierać odpowiednie środki ochrony technicznej i organizacyjnej. Posiada umiejętności wykorzystywania nowoczesnych narzędzi informatycznych, metod analizy danych oraz rozwiązań wspierających monitorowanie bezpieczeństwa i reagowanie na incydenty. Rozumie znaczenie bezpieczeństwa informacji w funkcjonowaniu współczesnych organizacji oraz wpływ nowych technologii na rozwój społeczeństwa cyfrowego i gospodarki opartej na wiedzy. Absolwent jest przygotowany do realizacji projektów informatycznych i pracy w zespołach specjalistycznych odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych. Potrafi samodzielnie oraz zespołowo planować i realizować złożone przedsięwzięcia projektowe, badawcze i rozwojowe z zakresu cyberbezpieczeństwa, formułować problemy badawcze, dobierać metody ich rozwiązywania i weryfikacji, analizować oraz interpretować uzyskane wyniki, a także wykorzystywać je do doskonalenia istniejących i opracowywania nowych rozwiązań. Potrafi efektywnie komunikować się z zespołami technicznymi oraz kadrą zarządzającą, a także prezentować wyniki analiz, badań i proponowane rozwiązania. Posiada kompetencje organizacyjne i społeczne umożliwiające funkcjonowanie w dynamicznie zmieniającym się środowisku technologicznym, w tym umiejętność samodzielnego uczenia się, rozwoju zawodowego oraz podejmowania odpowiedzialnych decyzji. Absolwent zna regulacje prawne, normy i standardy związane z ochroną danych, bezpieczeństwem informacji oraz funkcjonowaniem systemów teleinformatycznych. Rozumie znaczenie etyki zawodowej, odpowiedzialności społecznej oraz konieczności zachowania poufności, integralności i dostępności informacji. Dzięki praktycznemu profilowi studiów oraz realizowanym praktykom zawodowym posiada przygotowanie do efektywnego wykorzystania zdobytej wiedzy i umiejętności w środowisku pracy.

UZYSKIWANE KWALIFIKACJE ORAZ UPRAWNIENIA ZAWODOWE

Absolwent uzyskuje kwalifikacje umożliwiające wykonywanie zaawansowanych zadań zawodowych związanych z analizowaniem, projektowaniem, wdrażaniem, utrzymaniem oraz doskonaleniem systemów bezpieczeństwa teleinformatycznego. Dysponuje kompetencjami w zakresie projektowania architektury bezpieczeństwa złożonych systemów teleinformatycznych i organizacji, monitorowania bezpieczeństwa infrastruktury IT, analizy podatności i zagrożeń, reagowania na incydenty bezpieczeństwa oraz stosowania metod ochrony danych i systemów informatycznych. Zdobyte kwalifikacje obejmują również umiejętność prowadzenia analiz bezpieczeństwa, wspierania procesów audytowych, oceny i zarządzania ryzykiem oraz opracowywania i wdrażania polityk i procedur bezpieczeństwa informacji zgodnych z obowiązującymi standardami, regulacjami i wymaganiami organizacyjnymi. Absolwent potrafi planować i realizować przedsięwzięcia badawcze i rozwojowe w obszarze cyberbezpieczeństwa, formułować problemy badawcze, dobierać metody ich rozwiązywania i weryfikacji, analizować oraz interpretować uzyskane wyniki, a także wykorzystywać je do doskonalenia istniejących i opracowywania nowych rozwiązań. Absolwent jest przygotowany do pracy z nowoczesnymi narzędziami wspierającymi cyberbezpieczeństwo, systemami monitorowania bezpieczeństwa, rozwiązaniami wykorzystującymi analizę danych, sztuczną inteligencję i automatyzację procesów bezpieczeństwa oraz technologiami stosowanymi w ochronie infrastruktury informatycznej i infrastruktury krytycznej. Potrafi samodzielnie rozwiązywać złożone problemy związane z bezpieczeństwem systemów teleinformatycznych oraz efektywnie współpracować w zespołach projektowych, eksperckich i interdyscyplinarnych. Ukończenie studiów umożliwia podjęcie pracy na stanowiskach związanych z cyberbezpieczeństwem, bezpieczeństwem informacji, audytem bezpieczeństwa, projektowaniem i zarządzaniem architekturą bezpieczeństwa, administracją i zarządzaniem systemami IT, a także realizacją prac badawczo-rozwojowych w przedsiębiorstwach, instytucjach publicznych, sektorze usług informatycznych oraz jednostkach odpowiedzialnych za ochronę infrastruktury krytycznej. Absolwent jest również przygotowany do dalszego rozwoju zawodowego, zdobywania specjalistycznych certyfikatów branżowych, uczestnictwa w działalności badawczej i rozwojowej oraz kontynuowania kształcenia w szkole doktorskiej i innych formach kształcenia specjalistycznego.

PRAKTYKI ZAWODOWE

W programie studiów na kierunku Cyberbezpieczeństwo (studia drugiego stopnia) przewidziano obowiązkowe praktyki zawodowe realizowane w łącznym wymiarze 480 godzin lekcyjnych (360 godzin zegarowych) w dwóch semestrach studiów (I–II). Za realizację praktyk zawodowych student uzyskuje 14 punktów ECTS. Student realizuje zadania zawodowe w rzeczywistym środowisku pracy, uczestnicząc w działaniach związanych z bezpieczeństwem systemów teleinformatycznych pod nadzorem opiekuna z ramienia zakładu pracy. Dopuszcza się realizację praktyk w formie praktyki ciągłej, praktyki realizowanej równolegle ze studiami, a także w formie zatrudnienia, stażu lub działalności zawodowej pod warunkiem zgodności wykonywanych obowiązków z efektami uczenia się oraz ich zatwierdzenia przez kierownika praktyk.

Praktyki zawodowe umożliwiają osiągnięcie i weryfikację efektów uczenia się przypisanych do kierunku. Szczegółowe zasady organizacji i realizacji praktyk określa regulamin praktyk. Student zobowiązany jest do realizacji programu praktyk zgodnego z efektami uczenia się dla kierunku, wykonywania zadań właściwych dla profilu kształcenia, prowadzenia dokumentacji praktyk, sporządzenia sprawozdania z ich przebiegu oraz uzyskania potwierdzenia odbycia praktyki i opinii opiekuna w zakładzie pracy. Zaliczenie praktyk następuje na podstawie zaświadczenia o odbyciu praktyki, opinii opiekuna z zakładu pracy oraz oceny dokumentacji przedstawionej przez studenta, w szczególności pod kątem stopnia osiągnięcia zakładanych efektów uczenia się. Ostateczną ocenę wystawia kierownik praktyk z ramienia uczelni. Praktyki odbywają się w przedsiębiorstwach, instytucjach lub organizacjach prowadzących działalność związaną z cyberbezpieczeństwem, bezpieczeństwem informacji, ochroną danych, administracją i zabezpieczaniem systemów teleinformatycznych, monitorowaniem zagrożeń oraz wdrażaniem i utrzymaniem rozwiązań służących ochronie infrastruktury IT i usług cyfrowych.

OPIS ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ

Opis zakładanych efektów uczenia się uwzględnia:

1. Uniwersalne charakterystyki pierwszego stopnia określone w załączniku do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji.
2. Charakterystyki drugiego stopnia określone w załączniku do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji w tym efektów uczenia się umożliwiających uzyskanie kompetencji inżynierskich.

Opis zakładanych efektów jest ujęty w trzech kategoriach:

WIEDZY (W):

- WG - zakres i głębia - kompletność perspektywy poznawczej i zależności
- WK - kontekst - uwarunkowania i skutki

UMIEJĘTNOŚCI (U):

- UW - wykorzystanie wiedzy - rozwiązywane problemy i wykonywane zadania
- UK - komunikowanie się - odbieranie i tworzenie wypowiedzi, upowszechnianie wiedzy w środowisku naukowym i posługiwanie się językiem obcym
- UO - organizacja pracy - planowanie i praca zespołowa
- UU - uczenie się - planowanie własnego rozwoju i rozwoju innych osób

KOMPETENCJI (K):

- KK - oceny - krytyczne podejście
- KO - odpowiedzialność - wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego
- KR - rola zawodowa - niezależność i rozwój etosu

EFEKTY UCZENIA SIĘ

Symbol efektu kierunkowego	Kierunkowe efekty uczenia się	Kod składnika opisu
	WIEDZA	
K_W01	Absolwent zna i rozumie mechanizmy współczesnych zagrożeń i ataków cybernetycznych oraz metody analizy podatności, identyfikacji zagrożeń i oceny ryzyka w środowiskach teleinformatycznych.	P7U_W P7S_WG
K_W02	Absolwent zna i rozumie w pogłębionym stopniu architekturę, zasady funkcjonowania oraz mechanizmy bezpieczeństwa współczesnych systemów komputerowych i sieci teleinformatycznych, w tym środowisk serwerowych, chmurowych, rozproszonych, wbudowanych, IoT oraz OT.	P7U_W P7S_WG inż_P7S_WG
K_W03	Absolwent zna i rozumie metody kryptografii stosowanej, steganografii oraz mechanizmy zapewniania bezpieczeństwa danych, w tym uwierzytelniania, autoryzacji i kontroli dostępu w systemach teleinformatycznych.	P7U_W P7S_WG inż_P7S_WG
K_W04	Absolwent zna i rozumie w pogłębionym stopniu zasady projektowania, programowania i zabezpieczania oprogramowania, aplikacji internetowych oraz interfejsów API, a także procesy i praktyki DevSecOps stosowane w cyklu życia nowoczesnych systemów informatycznych.	P7U_W P7S_WG inż_P7S_WG
K_W05	Absolwent zna i rozumie w pogłębionym stopniu zasady funkcjonowania centrów operacji bezpieczeństwa (SOC), metody monitorowania i analizy bezpieczeństwa systemów teleinformatycznych, analizy logów, reagowania na incydenty oraz informatyki śledczej, a także techniki threat intelligence i threat hunting stosowane w identyfikacji i analizie zagrożeń cybernetycznych.	P7U_W P7S_WG
K_W06	Absolwent zna i rozumie w pogłębionym stopniu metody audytu i testowania bezpieczeństwa systemów teleinformatycznych, zasady oceny zgodności oraz mechanizmy zarządzania bezpieczeństwem informacji, w tym systemy ISMS, wymagania compliance oraz procedury zapewniania ciągłości działania organizacji.	P7U_W P7S_WG inż_P7S_WG
K_W07	Absolwent zna i rozumie w pogłębionym stopniu metody analityczne i optymalizacyjne, techniki uczenia maszynowego oraz sztucznej inteligencji, a także metody analizy danych, przetwarzania języka naturalnego i dużych modeli językowych wykorzystywane w cyberbezpieczeństwie, w tym do wykrywania anomalii, analizy zagrożeń i wspomagania procesów ochrony systemów teleinformatycznych.	P7U_W P7S_WG inż_P7S_WG
K_W08	Absolwent zna i rozumie zasady planowania, projektowania i realizacji projektów inżynierskich oraz przedsięwzięć z zakresu cyberbezpieczeństwa, a także metodykę prowadzenia badań i prac rozwojowych, obejmującą formułowanie problemów, dobór metod ich rozwiązywania i weryfikacji oraz analizę i interpretację wyników. Zna i rozumie zasady przygotowywania opracowań naukowych i technicznych, wdrażania i rozwoju rozwiązań w obszarze bezpieczeństwa systemów teleinformatycznych oraz podstawowe uwarunkowania tworzenia i rozwoju różnych form przedsiębiorczości.	P7U_W P7S_WG P7S_WK inż._P7S_WG
K_W09	Absolwent zna i rozumie prawne, organizacyjne, ekonomiczne, społeczne, etyczne i komunikacyjne uwarunkowania cyberbezpieczeństwa oraz cyberprzestępczości, w tym zasady ochrony własności intelektualnej, bezpieczeństwa informacji i odpowiedzialności zawodowej, a także zagadnienia związane z bezpiecznym, odpowiedzialnym i zgodnym z regulacjami wykorzystywaniem technologii informatycznych oraz wdrażaniem i komercjalizacją rozwiązań IT.	P7U_W P7S_WK
K_W10	Absolwent zna i rozumie fundamentalne dylematy współczesnej cywilizacji cyfrowej i komunikacji społecznej, związane z rozwojem technologii informacyjnych, sztucznej inteligencji, prywatności, bezpieczeństwa, dezinformacji oraz wpływu technologii na społeczeństwo i gospodarkę.	P7U_W P7S_WG P7S_WK
K_W11	Absolwent zna i rozumie specjalistyczną terminologię anglojęzyczną właściwą dla cyberbezpieczeństwa i informatyki oraz jej zastosowanie w dokumentacji technicznej, komunikacji zawodowej i analizie literatury specjalistycznej.	P7U_W P7S_WG P7S_WK

	UMIEJĘTNOŚCI	
K_U01	Absolwent potrafi identyfikować zagrożenia, analizować podatności oraz modelować scenariusze ataków cybernetycznych, a także oceniać ryzyko dla systemów teleinformatycznych, sieci, aplikacji i procesów organizacyjnych.	P7U_U P7S_UW
K_U02	Absolwent potrafi analizować wymagania bezpieczeństwa, projektować architekturę bezpieczeństwa złożonych systemów teleinformatycznych i organizacji oraz wdrażać, konfigurować i integrować mechanizmy bezpieczeństwa w systemach komputerowych i sieciach teleinformatycznych, w tym w środowiskach chmurowych, rozproszonych, wbudowanych oraz Internetu rzeczy (IoT).	P7U_U P7S_UW inż_P7S_UW
K_U03	Absolwent potrafi dobierać i stosować mechanizmy kryptograficzne, steganograficzne oraz rozwiązania służące ochronie danych, uwierzytelnianiu użytkowników, autoryzacji i kontroli dostępu w systemach teleinformatycznych.	P7U_U P7S_UW inż_P7S_UW
K_U04	Absolwent potrafi projektować, implementować, analizować i zabezpieczać oprogramowanie, aplikacje internetowe oraz interfejsy API, a także wspierać bezpieczny cykl życia oprogramowania z wykorzystaniem praktyk DevSecOps.	P7U_U P7S_UW inż_P7S_UW
K_U05	Absolwent potrafi monitorować bezpieczeństwo systemów teleinformatycznych, analizować logi i zdarzenia bezpieczeństwa, korelować alerty oraz wykorzystywać narzędzia SOC do wykrywania i analizy incydentów cyberbezpieczeństwa.	P7U_U P7S_UW inż_P7S_UW
K_U06	Absolwent potrafi reagować na incydenty cyberbezpieczeństwa, prowadzić podstawową analizę śledczą i analizę powłamaniową, dokumentować przebieg incydentu oraz proponować działania naprawcze i prewencyjne.	P7U_U P7S_UW
K_U07	Absolwent potrafi przeprowadzać audyty bezpieczeństwa, testy penetracyjne oraz oceny zgodności i efektywności mechanizmów ochrony systemów teleinformatycznych, a także analizować i interpretować wyniki tych działań.	P7U_U P7S_UW inż_P7S_UW
K_U08	Absolwent potrafi wykorzystywać metody analizy danych, optymalizacji, uczenia maszynowego, sztucznej inteligencji oraz wizualizacji danych do wspomagania procesów cyberobrony i analizy zagrożeń cybernetycznych.	P7U_U P7S_UW inż_P7S_UW
K_U09	Absolwent potrafi opracowywać polityki bezpieczeństwa, procedury, raporty oraz dokumentację techniczną i organizacyjną, a także komunikować wyniki analiz i rekomendacje zarówno specjalistom, jak i odbiorcom nietechnicznym.	P7U_U P7S_UW
K_U10	Absolwent potrafi planować i prowadzić analizy oraz przedsięwzięcia badawcze z zakresu cyberbezpieczeństwa, dobierać metody weryfikacji i oceny bezpieczeństwa, interpretować uzyskane wyniki oraz formułować rekomendacje dotyczące ochrony systemów i danych.	P7U_U P7S_UW
K_U11	Absolwent potrafi pracować indywidualnie i zespołowo nad złożonym przedsięwzięciem z zakresu cyberbezpieczeństwa, określać wymagania, planować zadania, zarządzać zakresem prac oraz komunikować decyzje projektowe interesariuszom.	P7U_U P7S_UO inż_P7S_UW
K_U12	Absolwent potrafi komunikować się w środowisku zawodowym i społecznym, także w języku obcym na poziomie B2+, przygotowywać wypowiedzi i opracowania specjalistyczne oraz stosować zasady bezpieczeństwa i higieny pracy.	P7U_U; P7S_UK
K_U13	Absolwent potrafi samodzielnie aktualizować wiedzę, planować własny rozwój, korzystać z literatury, dokumentacji technicznej i źródeł branżowych oraz rozwiązywać nowe problemy techniczne z wykorzystaniem krytycznej analizy informacji.	P7U_U; P7S_UU
K_U14	Absolwent potrafi integrować wiedzę z różnych obszarów cyberbezpieczeństwa i informatyki w celu projektowania, implementacji i wdrażania złożonych rozwiązań służących ochronie systemów teleinformatycznych, oceniając ich skuteczność, ograniczenia, konsekwencje etyczne i społeczne oraz możliwości rozwoju.	P7U_U; P7S_UW inż_P7S_UW
	KOMPETENCJE	
K_K01	Absolwent jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści, uznawania znaczenia wiedzy oraz opinii ekspertów w rozwiązywaniu problemów poznawczych i praktycznych, a także do odpowiedzialnego podejmowania decyzji zawodowych, pełnienia ról zawodowych zgodnie z zasadami etyki, bezpieczeństwa i rzetelności inżynierskiej oraz dbania o dorobek i rozwój zawodu informatyka i specjalisty cyberbezpieczeństwa.	P7U_K P7S_KK P7S_KR
K_K02	Absolwent jest przygotowany do współpracy w zespołach interdyscyplinarnych, przyjmowania różnych ról projektowych, komunikowania się z interesariuszami oraz ponoszenia odpowiedzialności za powierzone zadania.	P7U_K P7S_KO

K_K03	Absolwent rozumie potrzebę ciągłego rozwoju zawodowego i samokształcenia, śledzenia rozwoju technologii informatycznych oraz uwzględniania społecznych, prawnych i gospodarczych skutków projektowanych rozwiązań informatycznych.	P7U_K P7S_KR P7S_KO

MATRYCA ODNIESIEŃ EFEKTÓW WIEDZY DO UMIEJĘTNOŚCI

Umiejętności/Wiedza	K_W01	K_W02	K_W03	K_W04	K_W05	K_W06	K_W07	K_W08	K_W09	K_W10	K_W11
K_U01	1				1		1				
K_U02		1	1								
K_U03			1								
K_U04				1							
K_U05	1	1			1		1				
K_U06	1				1						
K_U07	1			1		1					
K_U08							1				
K_U09					1	1			1	1	1
K_U10	1					1	1	1			
K_U11				1		1		1	1		
K_U12									1	1	1
K_U13								1	1	1	1
K_U14		1	1	1				1			

MATRYCA POKRYCIA EFEKTÓW KIERUNKOWYCH

PRZEDMIOT	sem	K_W01	K_W02	K_W03	K_W04	K_W05	K_W06	K_W07	K_W08	K_W09	K_W10	K_W11	K_U01	K_U02	K_U03	K_U04	K_U05	K_U06	K_U07	K_U08	K_U09	K_U10	K_U11	K_U12	K_U13	K_U14	K_K01	K_K02	K_K03
Szkolenie biblioteczne	1											1													1				1
Szkolenie BHK	1									1														1			1		
Kryptografia stosow. i ochrona danych	1			1											1						1						1		
Zaaw. technol. zab. infrastr. sieciowej	1		1	1										1	1											1	1		
Steganogr. i ochrona informacji ukrytej	1			1											1							1				1		
Bezp. systemów serwerowych	1		1				1							1			1		1								1		
Proj. i inżynieria syst.informatycznych	1				1				1							1							1			1		1	
Czynnik ludzki, kultura bezp.i komun. kryzys.	1									1	1										1			1			1	1	
Reagowanie na inc. i informatyka śledcza	1	1				1							1				1	1			1						1	1	
Bezpieczeństwo aplikacji i DevSecOps	1				1											1			1				1			1	1	1	
Programow. system. i współbieżne w Rust	1				1											1									1	1			1
Tworz. nowoczesnych aplikacji internet.i API	1				1											1										1		1	
Praktyka zawodowa	1	1	1		1	1	1		1				1	1		1	1	1	1		1	1	1		1	1	1	1	1
J.ang. dla potrzeb rynku pracy B2+	2											1									1			1	1			1	1
SOC i monitoring bezpieczeństwa	2					1											1	1			1						1	1	
Bezp. chmury i środ. Rozpr.(t. Blockchain)	2		1	1										1	1											1			1
Audyt bezpieczeństwa i testy penetracyjne	2	1					1						1						1		1	1					1	1	
Realiz. i zarządzanie przedsięwz. inż.	2								1	1											1	1	1					1	1
Seminarium dyplomowe 1	2								1													1	1		1	1			1
Zaaw. metody optymal. syst. komp.	2		1					1												1		1				1			1
AI i detekcja anomalii w cyberbezp.	2	1				1		1					1				1			1		1						1		1
Threat intelligence i threat hunting	2	1				1							1				1	1			1						1	1	
Zaaw. metody uczenia maszynowego	2							1												1		1			1	1			1
Programow. Internetu Rzeczy i syst. wbud.	2		1		1									1		1										1			1
Wizualizacja danych i komunik. wyników	2							1	1											1	1			1				1	
Praktyka zawodowa	2	1	1		1	1	1		1				1	1		1	1	1	1		1	1	1		1	1	1	1	1
Prawo i normy w cyberbezpieczeństwie	3						1			1	1								1		1			1			1		1
Cyberprzestrzeń i cyberprzestępczość	3	1								1	1		1								1			1			1		1
Metody badawcze w naukach inż.-techn.	3							1	1											1		1			1				1
Seminarium dyplomowe 2	3								1													1			1	1			1
Zarz. ryzykiem, ISMS i ciągłość działania	3	1					1			1			1						1		1		1				1	1	
Bezp. infrastruktury krytycznej, OT i IoT	3	1	1				1						1	1					1							1	1		
Met.inż. i komercjaliz. w branży IT	3								1	1												1	1			1		1	1
Wykł. mon.: zagr. i trendy w cyberbezp.	3	1						1			1		1							1					1				1
Przetwarzanie języka naturalnego	3							1			1									1	1			1					1
Programow. na GPU i obliczenia równoległe	3				1			1												1					1	1			1
Projekt. aplik. z wyk. dużych mod. język.	3				1			1			1					1				1	1					1			1
Analiza wydajności i niezawod. Systemów	3		1					1	1											1		1				1			1
Praca dyplomowa	3								1													1			1	1	1		1
Liczba przypisań do kursów		**10**	**9**	**4**	**9**	**6**	**7**	**10**	**11**	**7**	**6**	**2**	**10**	**7**	**4**	**8**	**7**	**5**	**8**	**10**	**16**	**14**	**8**	**7**	**12**	**19**	**19**	**15**	**23**

SPOSOBY WERYFIKACJI I OCENY EFEKTÓW UCZENIA SIĘ

Weryfikacja i ocena efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu kształcenia odbywa się w sposób ciągły, na poziomie poszczególnych zajęć oraz całego programu studiów. Na poziomie zajęć stosowane są zróżnicowane metody weryfikacji, dostosowane do rodzaju zajęć oraz zakładanych efektów uczenia się, w szczególności egzaminy pisemne i ustne, kolokwia, projekty indywidualne i zespołowe, zadania praktyczne, sprawozdania, prezentacje oraz ocena aktywności na zajęciach. Szczegółowe zasady weryfikacji i kryteria oceny określone są w sylabusach poszczególnych zajęć, a studenci są z nimi zapoznawani na początku realizacji zajęć. Warunkiem zaliczenia zajęć jest osiągnięcie zakładanych efektów uczenia się, potwierdzone uzyskaniem pozytywnej oceny z egzaminu lub zaliczenia oraz spełnieniem wymagań przewidzianych dla poszczególnych form zajęć, w tym ćwiczeń, laboratoriów, projektów i seminariów. Weryfikacja efektów uczenia się w zakresie umiejętności i kompetencji społecznych odbywa się w szczególności poprzez realizację projektów, prac zespołowych oraz zadań praktycznych, umożliwiających ocenę umiejętności rozwiązywania problemów, pracy w zespole oraz organizacji pracy. Na poziomie całego cyklu kształcenia osiągnięcie efektów uczenia się potwierdzane jest poprzez zaliczenie wszystkich etapów studiów oraz przygotowanie pracy dyplomowej (magisterskiej), stanowiącej rozwiązanie określonego problemu badawczego lub praktycznego, a także zdanie egzaminu dyplomowego. Przyjęte metody weryfikacji umożliwiają ocenę stopnia osiągnięcia efektów uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych. Część efektów uczenia się może być osiągana i weryfikowana w ramach zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość.

TREŚCI PROGRAMOWE ORAZ EFEKTY KIERUNKOWE

MODUŁ OGÓLNOUCZELNIANY	EFEKTY KIERUNKOWE
Szkolenie biblioteczne (semestr 1): Szkolenie ma na celu przygotowanie studentów do sprawnego korzystania z zasobów i usług biblioteki uczelnianej. Realizowane treści dotyczą organizacji biblioteki, zasad udostępniania zbiorów, metod wyszukiwania informacji naukowej w katalogach i bazach danych oraz korzystania z elektronicznych źródeł informacji niezbędnych w procesie studiowania i przygotowywania prac zaliczeniowych oraz dyplomowych.	K_W11 K_U13 K_K03
Szkolenie BHK (semestr 1): W ramach szkolenia studenci zapoznają się z podstawowymi zasadami bezpieczeństwa i higieny obowiązującymi podczas zajęć dydaktycznych, ćwiczeń, laboratoriów oraz pobytu na terenie uczelni. Omawiane są prawa i obowiązki studenta w zakresie bezpiecznego uczestnictwa w zajęciach, zasady postępowania w sytuacjach zagrożenia, ewakuacji oraz zgłaszania wypadków i niebezpiecznych zdarzeń. Poruszana jest również problematyka zagrożeń mogących występować w salach dydaktycznych, pracowniach specjalistycznych i laboratoriach, a także zasady korzystania z urządzeń, sprzętu i środków ochrony. Szkolenie obejmuje ponadto podstawowe zasady udzielania pierwszej pomocy oraz postępowania w stanach nagłego zagrożenia zdrowia lub życia.	K_W09 K_U12 K_K01
Język angielski dla potrzeb rynku pracy B2+ (semestr 2): W ramach zajęć studenci rozwijają kompetencje językowe na poziomie B2+ w kontekście rynku pracy, ze szczególnym uwzględnieniem komunikacji zawodowej. Studenci doskonalą umiejętności rozumienia i tworzenia wypowiedzi ustnych i pisemnych, w tym przygotowywania dokumentów aplikacyjnych, prowadzenia rozmów kwalifikacyjnych oraz komunikacji w środowisku pracy. W trakcie zajęć rozwijane są umiejętności pracy z tekstami specjalistycznymi oraz posługiwania się językiem angielskim w sytuacjach zawodowych, w tym podczas prezentacji, spotkań i pracy zespołowej.	K_W11 K_U09, K_U12, K_U13 K_K02, K_K03
MODUŁ KIERUNKOWY	**EFEKTY KIERUNKOWE**
Kryptografia stosowana i ochrona danych (semestr 1): W ramach kursu studenci pogłębiają wiedzę z zakresu kryptografii stosowanej oraz ochrony danych w systemach informatycznych. Omawiane są współczesne mechanizmy kryptograficzne, w tym szyfrowanie symetryczne i asymetryczne, funkcje skrótu, podpis cyfrowy, infrastruktura klucza publicznego (PKI) oraz protokoły zapewniające poufność, integralność i uwierzytelnianie danych. Szczególną uwagę poświęca się doborowi odpowiednich mechanizmów kryptograficznych do konkretnych scenariuszy bezpieczeństwa, a także analizie ograniczeń i błędów występujących podczas ich wdrażania. Kurs rozwija umiejętności praktycznego wykorzystania narzędzi kryptograficznych w procesie ochrony informacji i budowy bezpiecznych systemów informatycznych.	K_W03 K_U03, K_U09 K_K01
Zaawansowane technologie zabezpieczania infrastruktury sieciowej (semestr 1): W ramach kursu studenci zdobywają wiedzę dotyczącą nowoczesnych protokołów komunikacyjnych oraz mechanizmów bezpieczeństwa stosowanych w sieciach komputerowych. Omawiane są zagadnienia związane z ochroną transmisji danych, segmentacją sieci, kontrolą dostępu, tunelowaniem, wirtualnymi sieciami prywatnymi (VPN) oraz mechanizmami monitorowania i filtrowania ruchu sieciowego. Szczególną uwagę poświęca się identyfikacji zagrożeń wynikających z błędnej konfiguracji usług sieciowych oraz niewłaściwego zarządzania infrastrukturą teleinformatyczną. Kurs rozwija umiejętność oceny poziomu bezpieczeństwa rozwiązań sieciowych, analizy potencjalnych zagrożeń oraz doboru adekwatnych mechanizmów ochrony w zależności od specyfiki środowiska i wymagań bezpieczeństwa.	K_W02, K_W03 K_U02, K_U03, K_U14 K_K01
Steganografia i ochrona informacji ukrytej (semestr 1): W ramach kursu studenci poznają metody steganografii oraz zagadnienia związane z ochroną informacji ukrytej w systemach cyfrowych. Omawiane są techniki osadzania danych w obrazach, plikach dźwiękowych oraz innych nośnikach informacji, a także metody wykrywania i analizy ukrytych przekazów. Zajęcia obejmują również problematykę kanałów ukrytych, ocenę skuteczności stosowanych technik oraz analizę zagrożeń wynikających z wykorzystania steganografii w działalności przestępczej, szpiegowskiej i operacjach dezinformacyjnych. Kurs rozwija umiejętność identyfikowania, analizowania oraz projektowania rozwiązań związanych z ochroną informacji ukrytej i przeciwdziałaniem nieuprawnionemu wykorzystaniu technik steganograficznych.	K_W03 K_U03, K_U10 K_K01

Bezpieczeństwo systemów serwerowych (semestr 1): W ramach kursu studenci zdobywają wiedzę i umiejętności związane z zabezpieczaniem systemów serwerowych wykorzystywanych w organizacjach oraz usługach sieciowych. Omawiane są zagadnienia dotyczące konfiguracji usług serwerowych, zarządzania kontami użytkowników i uprawnieniami, aktualizacji oprogramowania, tworzenia kopii zapasowych, monitorowania pracy systemów oraz rejestrowania zdarzeń. Szczególną uwagę poświęca się metodom wzmacniania bezpieczeństwa systemów (hardening), identyfikacji typowych podatności serwerów oraz analizie błędów administracyjnych mogących prowadzić do naruszenia bezpieczeństwa. Kurs rozwija umiejętność praktycznej konfiguracji, administracji i utrzymania bezpiecznego środowiska serwerowego zgodnie z aktualnymi wymaganiami i dobrymi praktykami cyberbezpieczeństwa.	K_W02, K_W06 K_U02, K_U05, K_U07 K_K01
Projektowanie i inżynieria systemów informatycznych (semestr 1): W ramach kursu studenci rozwijają umiejętności projektowania, implementowania i oceny systemów informatycznych z uwzględnieniem wymagań funkcjonalnych, niefunkcjonalnych oraz jakościowych. Zakres obejmuje projektowanie architektury aplikacji, zarządzanie cyklem życia oprogramowania, metody testowania i zapewniania jakości, utrzymanie systemów informatycznych oraz wybrane praktyki inżynierii oprogramowania i DevOps. Omawiane są również zagadnienia związane z dokumentowaniem rozwiązań, automatyzacją procesów wytwórczych oraz podejmowaniem decyzji projektowych w złożonych środowiskach informatycznych. Kurs przygotowuje do świadomego projektowania i rozwijania systemów informatycznych oraz efektywnej pracy nad złożonymi przedsięwzięciami programistycznymi.	K_W04, K_W08 K_U04, K_U11, K_U14 K_K02
Czynnik ludzki, kultura bezpieczeństwa i komunikacja kryzysowa (semestr 1): W ramach kursu studenci poznają znaczenie czynnika ludzkiego w systemie cyberbezpieczeństwa oraz rolę kultury bezpieczeństwa w funkcjonowaniu organizacji. Omawiane są zagadnienia związane z błędami użytkowników, technikami socjotechnicznymi, komunikacją ryzyka, zachowaniami w sytuacjach kryzysowych oraz metodami budowania i wzmacniania świadomości bezpieczeństwa. Szczególną uwagę poświęca się problemom komunikacji pomiędzy zespołami technicznymi, kadrą zarządzającą i użytkownikami końcowymi, a także sposobom skutecznego przekazywania informacji dotyczących zagrożeń i zasad bezpieczeństwa. Kurs rozwija umiejętność formułowania jasnych i zrozumiałych komunikatów oraz wspierania odpowiedzialnych postaw i zachowań w środowisku cyfrowym.	K_W09, K_W10 K_U09, K_U12 K_K01, K_K02
SOC i monitoring bezpieczeństwa (semestr 2): W ramach kursu studenci zdobywają wiedzę i umiejętności związane z procesami oraz narzędziami wykorzystywanymi w Centrum Operacji Bezpieczeństwa (Security Operations Center - SOC). Omawiane są zagadnienia dotyczące monitorowania zdarzeń bezpieczeństwa, analizy logów, korelacji alertów, klasyfikacji incydentów, wykorzystania systemów SIEM oraz przygotowywania raportów operacyjnych. Szczególną uwagę poświęca się rolom analityków bezpieczeństwa, przepływowi informacji pomiędzy zespołami odpowiedzialnymi za bezpieczeństwo oraz procedurom eskalacji zdarzeń. Kurs rozwija umiejętność interpretowania sygnałów bezpieczeństwa, oceny ryzyka oraz podejmowania decyzji operacyjnych w środowisku ciągłego monitoringu i reagowania na incydenty..	K_W05 K_U05, K_U06, K_U09 K_K01, K_K02
Bezpieczeństwo chmury i środowisk rozproszonych (techn. Blockchain) (semestr 2): W ramach kursu studenci zdobywają wiedzę z zakresu bezpieczeństwa usług chmurowych, środowisk rozproszonych oraz technologii blockchain. Omawiane są modele odpowiedzialności w chmurze, zarządzanie tożsamością i dostępem, ochrona danych, bezpieczna konfiguracja usług, a także zagadnienia związane z bezpieczeństwem kontenerów i architektur rozproszonych. Zajęcia obejmują również podstawowe mechanizmy funkcjonowania technologii blockchain, inteligentnych kontraktów oraz analizę zagrożeń i ryzyk związanych z ich projektowaniem i wdrażaniem. Kurs rozwija umiejętność oceny poziomu bezpieczeństwa nowoczesnych środowisk infrastrukturalnych oraz doboru odpowiednich mechanizmów ochrony w zależności od specyfiki wykorzystywanych technologii.	K_W02, K_W03 K_U02, K_U03, K_U14 K_K03

Audyt bezpieczeństwa i testy penetracyjne (semestr 2): W ramach kursu studenci zdobywają wiedzę i umiejętności niezbędne do planowania oraz realizacji audytów bezpieczeństwa i testów penetracyjnych zgodnie z przyjętymi metodykami. Omawiane są zagadnienia związane z rozpoznaniem środowiska, identyfikacją podatności, doborem odpowiednich narzędzi, weryfikacją uzyskanych wyników, oceną ryzyka oraz przygotowaniem raportów zawierających rekomendacje działań naprawczych. Szczególną uwagę poświęca się aspektom etycznym, ograniczeniom prawnym i organizacyjnym oraz odpowiedzialności osób prowadzących działania audytowe i testy bezpieczeństwa. Kurs rozwija praktyczną umiejętność oceny poziomu bezpieczeństwa systemów informatycznych oraz formułowania zaleceń służących podnoszeniu odporności organizacji na zagrożenia cybernetyczne.	K_W01, K_W06 K_U01, K_U07, K_U09, K_U10 K_K01, K_K02
Realizacja i zarządzanie przedsięwzięciem inżynierskim (semestr 2): W ramach kursu studenci rozwijają umiejętności planowania, realizacji oraz kontroli przedsięwzięć inżynierskich w obszarze informatyki i cyberbezpieczeństwa. Omawiane są zagadnienia związane z definiowaniem celów projektowych, zarządzaniem zakresem, harmonogramem, zasobami, ryzykiem, jakością oraz komunikacją w projekcie. Szczególną uwagę poświęca się metodom organizacji pracy zespołowej, dokumentowania postępów realizacji zadań oraz skutecznego reagowania na zmieniające się wymagania i uwarunkowania projektowe. Kurs przygotowuje studentów do odpowiedzialnego prowadzenia i koordynowania złożonych przedsięwzięć technicznych w warunkach ograniczonych zasobów, presji czasu oraz zmieniających się potrzeb organizacyjnych.	K_W08, K_W09 K_U09, K_U10, K_U11 K_K02, K_K03
Seminarium dyplomowe 1 (semestr 2): W ramach zajęć studenci przygotowują koncepcję pracy dyplomowej oraz porządkują założenia problemu badawczo-inżynierskiego. Zakres seminarium obejmuje wybór tematu, analizę literatury przedmiotu, formułowanie celu i pytań badawczych, dobór metod badawczych oraz planowanie części projektowej lub praktycznej. Uczestnicy prezentują postępy prac, dyskutują proponowane rozwiązania oraz otrzymują informację zwrotną wspierającą doskonalenie przyjętych założeń i sposobu argumentacji. Seminarium rozwija umiejętność samodzielnego planowania i realizacji pracy dyplomowej, krytycznej analizy źródeł oraz profesjonalnego komunikowania wyników i założeń prowadzonych badań.	K_W08 K_U10, K_U11, K_U13, K_U14 K_K03
Prawo i normy w cyberbezpieczeństwie (semestr 3): W ramach zajęć studenci zapoznają się z regulacjami prawnymi, normami oraz wymaganiami zgodności obowiązującymi w obszarze cyberbezpieczeństwa. Analizowane są zagadnienia związane z ochroną danych, odpowiedzialnością prawną, wymaganiami organizacyjnymi, dokumentacją bezpieczeństwa, standardami branżowymi oraz podstawami zarządzania zgodnością. Omawiane są zależności pomiędzy przepisami prawa, politykami i procedurami organizacyjnymi a technicznymi mechanizmami ochrony informacji. Studenci uczą się identyfikować, interpretować i stosować wymagania compliance w praktyce zawodowej oraz uwzględniać je podczas projektowania, wdrażania i eksploatacji systemów informatycznych.	K_W06, K_W09, K_W10 K_U07, K_U09, K_U12 K_K01, K_K03
Cyberprzestrzeń i cyberprzestępczość (semestr 3): W ramach zajęć studenci poznają specyfikę funkcjonowania cyberprzestrzeni oraz zjawiska cyberprzestępczości w ujęciu technicznym, społecznym i prawnym. Analizowane są modele nadużyć cyfrowych, metody działania grup przestępczych, oszustwa internetowe, ataki wymierzone w użytkowników i organizacje oraz mechanizmy prowadzące do eskalacji zagrożeń. Omawiane są również podstawy analizy incydentów z uwzględnieniem aspektów odpowiedzialności, gromadzenia materiału dowodowego oraz skutków społecznych i organizacyjnych. Przedmiot rozwija umiejętność identyfikowania i oceny zagrożeń w cyberprzestrzeni oraz rozumienia ich szerszego kontekstu, wykraczającego poza aspekty techniczne.	K_W01, K_W09, K_W10 K_U01, K_U09, K_U12 K_K01, K_K03
Metody badawcze w naukach inżynieryjno-technicznych (semestr 3): W ramach kursu studenci zdobywają wiedzę i umiejętności niezbędne do planowania i prowadzenia badań oraz eksperymentów w obszarze informatyki i cyberbezpieczeństwa. Zakres obejmuje formułowanie problemów i pytań badawczych, dobór odpowiednich metod i narzędzi badawczych, projektowanie procedur eksperymentalnych, weryfikację hipotez, analizę i interpretację wyników oraz ocenę ich wiarygodności. Omawiane są również zasady przygotowywania opracowań naukowych i technicznych, dokumentowania przebiegu badań oraz prezentowania i dyskutowania uzyskanych rezultatów. Kurs rozwija umiejętność rzetelnego uzasadniania wniosków, krytycznej oceny wyników oraz stosowania metodologii badawczej w rozwiązywaniu problemów informatycznych i związanych z cyberbezpieczeństwem.	K_W07, K_W08 K_U08, K_U10, K_U13 K_K03

Seminarium dyplomowe 2 (semestr 3): W ramach zajęć studenci finalizują prace dyplomowe oraz przygotowują się do egzaminu dyplomowego. Seminarium obejmuje weryfikację struktury i kompletności pracy, doskonalenie części projektowej lub praktycznej, analizę i interpretację uzyskanych wyników, formułowanie wniosków oraz przygotowanie prezentacji rezultatów. Uczestnicy regularnie prezentują postępy prac, identyfikują obszary wymagające uzupełnienia i doskonalą sposób argumentacji naukowo-technicznej. Zajęcia wspierają rozwój umiejętności samodzielnego doprowadzenia projektu dyplomowego do zakończenia, krytycznej oceny uzyskanych rezultatów oraz skutecznego prezentowania i obrony przyjętych rozwiązań.	K_W08 K_U10, K_U13, K_U14 K_K03
MODUŁ KURSÓW OBIERALNYCH	**EFEKTY KIERUNKOWE**
Reagowanie na incydenty i informatyka śledcza (semestr 1) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z identyfikowaniem, analizowaniem oraz obsługą incydentów bezpieczeństwa w systemach informatycznych. Zakres obejmuje podstawy informatyki śledczej, metody zabezpieczania i analizowania śladów cyfrowych, identyfikację i interpretację zdarzeń bezpieczeństwa, a także procedury reagowania na incydenty i dokumentowania podejmowanych działań. Omawiane są również zasady zachowania integralności materiału dowodowego, analizy logów oraz przygotowywania raportów z przeprowadzonych działań. Kurs rozwija praktyczne umiejętności wykrywania naruszeń bezpieczeństwa, wspierania procesu zarządzania incydentami oraz prowadzenia podstawowych analiz powłamaniowych w środowiskach informatycznych.	K_W01, K_W05 K_U01, K_U05, K_U06, K_U09 K_K01, K_K02
Bezpieczeństwo aplikacji i DevSecOps (semestr 1) W ramach kursu studenci zapoznają się z metodami projektowania, testowania i utrzymywania bezpiecznych aplikacji w nowoczesnym cyklu wytwarzania oprogramowania. Zakres obejmuje identyfikację i analizę typowych podatności aplikacyjnych, projektowanie mechanizmów ochronnych, realizację testów bezpieczeństwa, automatyzację procesów kontroli jakości oraz wdrażanie praktyk DevSecOps. Omawiane są również zagadnienia związane z bezpiecznym cyklem życia oprogramowania, integracją wymagań bezpieczeństwa z procesami deweloperskimi oraz monitorowaniem bezpieczeństwa aplikacji po wdrożeniu. Kurs rozwija umiejętność uwzględniania wymagań bezpieczeństwa na wszystkich etapach projektowania, tworzenia, testowania i eksploatacji systemów informatycznych.	K_W04 K_U04, K_U07, K_U11, K_U14 K_K01, K_K02
Programowanie systemowe i współbieżne w Rust (semestr 1) W ramach kursu studenci rozwijają umiejętności tworzenia oprogramowania systemowego i współbieżnego z wykorzystaniem języka Rust. Zakres obejmuje zarządzanie pamięcią, model własności i pożyczania danych, bezpieczeństwo typów, programowanie współbieżne, komunikację między wątkami oraz projektowanie i implementację niezawodnych komponentów niskopoziomowych. Omawiane są również zagadnienia związane z optymalizacją wydajności, obsługą błędów oraz tworzeniem bezpiecznego i odpornego na awarie oprogramowania systemowego. Kurs przygotowuje do projektowania i implementacji wydajnych, niezawodnych i bezpiecznych rozwiązań działających blisko warstwy systemowej oraz wykorzystujących nowoczesne techniki programowania.	K_W04 K_U04, K_U13, K_U14 K_K03
Tworzenie nowoczesnych aplikacji internetowych i API (semestr 1) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z projektowaniem i implementowaniem współczesnych aplikacji internetowych oraz interfejsów programowania aplikacji (API). Zakres obejmuje architekturę aplikacji webowych, komunikację klient–serwer, projektowanie i implementację usług sieciowych, integrację z bazami danych, a także wybrane zagadnienia związane z bezpieczeństwem, testowaniem i utrzymaniem aplikacji. Omawiane są również metody zapewniania jakości, skalowalności i użyteczności rozwiązań internetowych. Kurs rozwija praktyczne umiejętności tworzenia, wdrażania i rozwijania aplikacji zgodnych z wymaganiami użytkowników oraz potrzebami organizacji.	K_W04 K_U04, K_U14 K_K02
Zaawansowane metody optymalizacji systemów komputerowych (semestr 2) W ramach kursu studenci pogłębiają umiejętności stosowania metod optymalizacji do analizy, projektowania i usprawniania działania systemów komputerowych. Zakres obejmuje modelowanie problemów z uwzględnieniem ograniczeń technicznych i organizacyjnych, definiowanie i dobór kryteriów jakości, analizę wydajności systemów oraz wykorzystanie wybranych technik optymalizacyjnych służących poprawie efektywności rozwiązań informatycznych. Omawiane są również metody oceny kompromisów pomiędzy wydajnością, niezawodnością, kosztami i wykorzystaniem zasobów. Kurs rozwija umiejętność łączenia wiedzy algorytmicznej i analitycznej z praktyczną oceną działania systemów oraz podejmowania decyzji prowadzących do zwiększenia efektywności infrastruktury informatycznej.	K_W02, K_W07 K_U08, K_U10, K_U14 K_K03

Sztuczna inteligencja i detekcja anomalii w cyberbezpieczeństwie (semestr 2) W ramach kursu studenci zapoznają się z zastosowaniami sztucznej inteligencji i uczenia maszynowego w wykrywaniu anomalii oraz zagrożeń cyberbezpieczeństwa. Zakres obejmuje przygotowanie i przetwarzanie danych, dobór i trenowanie modeli, ocenę jakości detekcji z wykorzystaniem odpowiednich metryk oraz interpretację wyników w kontekście identyfikacji i analizy zagrożeń. Omawiane są metody wykrywania nietypowych zachowań w ruchu sieciowym, aktywności użytkowników oraz zdarzeniach systemowych, a także ograniczenia i wyzwania związane z wykorzystaniem technik sztucznej inteligencji w środowiskach bezpieczeństwa. Kurs rozwija umiejętność stosowania metod analitycznych do rozpoznawania anomalii, wspierania procesu wykrywania zagrożeń oraz podejmowania decyzji w obszarze cyberbezpieczeństwa.	K_W01, K_W05, K_W07 K_U01, K_U05, K_U08, K_U10 K_K01, K_K03
Threat intelligence and threat hunting (semestr 2) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z wykorzystaniem informacji o zagrożeniach (threat intelligence) oraz aktywnym poszukiwaniem śladów kompromitacji w środowiskach informatycznych (threat hunting). Zakres obejmuje źródła i metody pozyskiwania informacji o zagrożeniach, analizę taktyk, technik i procedur stosowanych przez atakujących, identyfikację wskaźników kompromitacji i zachowań, formułowanie hipotez badawczych oraz ocenę ryzyka wynikającego z obserwowanych zdarzeń i anomalii. Omawiane są również sposoby korelacji danych pochodzących z różnych źródeł oraz wykorzystania informacji o zagrożeniach w procesach monitorowania, wykrywania i reagowania na incydenty bezpieczeństwa. Kurs rozwija umiejętność analizy zagrożeń, krytycznej oceny dostępnych informacji oraz ich odpowiedzialnego wykorzystania w działaniach służących ochronie organizacji.	K_W01, K_W05 K_U01, K_U05, K_U06, K_U09 K_K01, K_K02
Zaawansowane metody uczenia maszynowego (semestr 2) W ramach kursu studenci pogłębiają wiedzę i umiejętności związane ze stosowaniem zaawansowanych metod uczenia maszynowego w rozwiązywaniu problemów informatycznych. Zakres obejmuje przygotowanie i przetwarzanie danych, dobór i trenowanie modeli, walidację i ocenę jakości uzyskiwanych wyników, interpretację rezultatów oraz analizę ograniczeń i ryzyk związanych z wykorzystaniem metod predykcyjnych. Omawiane są zarówno zagadnienia związane z uczeniem nadzorowanym i nienadzorowanym, jak i metody wspierające poprawę jakości, wiarygodności i interpretowalności modeli. Kurs rozwija umiejętność krytycznej oceny modeli uczenia maszynowego, świadomego doboru metod analitycznych oraz ich efektywnego wykorzystania do rozwiązywania złożonych problemów informatycznych.	K_W07 K_U08, K_U10, K_U14 K_K03
Programowanie Internetu rzeczy i systemów wbudowanych (semestr 2) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z projektowaniem i programowaniem rozwiązań Internetu Rzeczy (IoT – Internet of Things) oraz systemów wbudowanych. Zakres obejmuje architekturę urządzeń, komunikację i wymianę danych, zarządzanie ograniczonymi zasobami sprzętowymi, zapewnianie niezawodności działania, bezpieczeństwo urządzeń i komunikacji oraz integrację z systemami nadrzędnymi i usługami sieciowymi. Omawiane są również zagadnienia związane z monitorowaniem, diagnostyką i eksploatacją rozwiązań IoT w rzeczywistych środowiskach. Kurs rozwija umiejętność projektowania, implementacji i oceny praktycznych rozwiązań integrujących warstwę sprzętową, programową i sieciową w celu realizacji określonych funkcji użytkowych.	K_W02, K_W04 K_U02, K_U04, K_U14 K_K03
Wizualizacja danych i komunikacja wyników (semestr 2) W ramach kursu studenci rozwijają umiejętności prezentowania danych oraz wyników analiz w sposób czytelny, rzetelny i dostosowany do potrzeb różnych grup odbiorców. Zakres obejmuje metody wizualizacji danych, dobór odpowiednich form prezentacji, projektowanie wykresów, raportów i dashboardów, interpretację wyników analiz oraz zasady skutecznego komunikowania wniosków technicznych i biznesowych. Omawiane są również zagadnienia związane z poprawnością przekazu, unikanie błędów interpretacyjnych oraz etyczne aspekty prezentacji danych. Kurs rozwija umiejętność łączenia analizy danych z odpowiedzialną komunikacją rezultatów, wspierającą procesy decyzyjne w organizacjach.	K_W07, K_W08 K_U08, K_U09, K_U12 K_K02

Zarządzanie ryzykiem, ISMS i ciągłość działania (semestr 3) W ramach kursu studenci zapoznają się z metodami zarządzania ryzykiem informacyjnym oraz zasadami organizacji i doskonalenia systemu zarządzania bezpieczeństwem informacji. Zakres obejmuje identyfikację i klasyfikację aktywów, analizę zagrożeń i podatności, ocenę ryzyka, dobór i wdrażanie zabezpieczeń, planowanie ciągłości działania, dokumentowanie decyzji oraz zapewnianie zgodności z wymaganiami organizacyjnymi, prawnymi i regulacyjnymi. Omawiane są również zagadnienia związane z monitorowaniem skuteczności zabezpieczeń, zarządzaniem incydentami oraz ciągłym doskonaleniem procesów bezpieczeństwa. Kurs rozwija umiejętność integrowania technicznych i organizacyjnych aspektów ochrony informacji oraz podejmowania decyzji wspierających bezpieczeństwo i odporność organizacji.	K_W01, K_W06, K_W09 K_U01, K_U07, K_U09, K_U11 K_K01, K_K02
Bezpieczeństwo infrastruktury krytycznej, OT i IoT (semestr 3) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z analizą bezpieczeństwa systemów infrastruktury krytycznej, środowisk technologii operacyjnej (OT – Operational Technology) oraz rozwiązań Internetu Rzeczy (IoT – Internet of Things). Zakres obejmuje specyfikę systemów przemysłowych i wbudowanych, identyfikację podatności, modelowanie zagrożeń, ocenę ryzyka oraz dobór i ocenę skuteczności mechanizmów ochrony. Omawiane są również zagadnienia związane z bezpieczeństwem komunikacji, segmentacją sieci, monitorowaniem środowisk przemysłowych oraz zapewnianiem ciągłości działania i odporności operacyjnej. Kurs rozwija umiejętność projektowania, wdrażania i oceny zabezpieczeń w środowiskach charakteryzujących się podwyższonymi wymaganiami w zakresie niezawodności, dostępności i bezpieczeństwa.	K_W01, K_W02, K_W06 K_U01, K_U02, K_U07, K_U14 K_K01
Metody inżynierskie i komercjalizacja w branży IT (semestr 3) W ramach kursu studenci poznają zależności pomiędzy metodami inżynierskimi, procesem tworzenia rozwiązań informatycznych oraz ich wdrażaniem i komercjalizacją w branży IT. Zakres obejmuje analizę potrzeb interesariuszy, ocenę wykonalności technicznej i organizacyjnej przedsięwzięć, opracowywanie koncepcji produktów i usług informatycznych, budowę modeli biznesowych, identyfikację ryzyk wdrożeniowych oraz podstawy ochrony rezultatów pracy intelektualnej. Omawiane są również metody prezentowania wartości technicznej, użytkowej i biznesowej proponowanych rozwiązań. Kurs rozwija umiejętność integrowania perspektywy technicznej, organizacyjnej i rynkowej w procesie projektowania, wdrażania i rozwoju innowacyjnych produktów informatycznych.	K_W08, K_W09 K_U10, K_U11, K_U14 K_K02, K_K03
Wykład monograficzny: zagrożenia i trendy w cyberbezpieczeństwie (semestr 3) W ramach wykładu monograficznego studenci zapoznają się z aktualnymi zagrożeniami, technologiami oraz trendami w obszarze cyberbezpieczeństwa na podstawie najnowszych przykładów branżowych, raportów i studiów przypadków. Zakres tematyczny może obejmować nowe modele i techniki ataków, zmiany regulacyjne i standardy bezpieczeństwa, rozwój narzędzi ofensywnych i defensywnych, bezpieczeństwo systemów wykorzystujących sztuczną inteligencję oraz ewolucję infrastruktury cyfrowej. Treści wykładu są na bieżąco aktualizowane i dostosowywane do kierunków rozwoju dyscypliny naukowej oraz potrzeb rynku pracy. Kurs rozwija umiejętność krytycznej analizy nowych zjawisk, oceny ich wpływu na bezpieczeństwo systemów informatycznych oraz identyfikowania wyzwań i szans związanych z rozwojem technologii cyfrowych.	K_W01, K_W07, K_W10 K_U01, K_U08, K_U13 K_K03
Przetwarzanie języka naturalnego (semestr 3) W ramach kursu studenci zapoznają się z metodami przetwarzania języka naturalnego (NLP - Natural Language Processing) oraz ich zastosowaniami w systemach informatycznych. Zakres obejmuje reprezentację i przygotowanie danych tekstowych, przetwarzanie i analizę języka naturalnego, modelowanie danych językowych, ocenę jakości uzyskiwanych wyników oraz wykorzystanie wybranych narzędzi i technik NLP. Omawiane są również praktyczne zastosowania metod przetwarzania języka naturalnego w analizie dokumentów, automatycznej klasyfikacji treści, wyszukiwaniu informacji oraz wspomaganiu procesów decyzyjnych. Kurs rozwija umiejętność stosowania metod sztucznej inteligencji do analizy, interpretacji i przetwarzania informacji tekstowej w różnorodnych zastosowaniach informatycznych.	K_W07, K_W10 K_U08, K_U09, K_U12 K_K03

Programowanie na GPU i obliczenia równoległe (semestr 3) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z wykorzystaniem obliczeń równoległych oraz akceleracji z użyciem procesorów graficznych (GPU – Graphics Processing Unit) w rozwiązywaniu złożonych problemów obliczeniowych. Zakres obejmuje modele programowania równoległego, organizację i synchronizację obliczeń, zarządzanie pamięcią, analizę wydajności aplikacji oraz ocenę ograniczeń wynikających z architektury sprzętowej. Omawiane są również metody optymalizacji algorytmów oraz zastosowania obliczeń równoległych w analizie danych, symulacjach komputerowych, sztucznej inteligencji i innych zadaniach wymagających dużej mocy obliczeniowej. Kurs rozwija umiejętność projektowania, implementacji i oceny wydajnych rozwiązań wykorzystujących nowoczesne architektury obliczeniowe.	K_W04, K_W07 K_U08, K_U13, K_U14 K_K03
Projektowanie aplikacji z wykorzystaniem dużych modeli językowych (semestr 3) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z projektowaniem aplikacji wykorzystujących duże modele językowe (LLM – Large Language Models) oraz narzędzia sztucznej inteligencji generatywnej. Zakres obejmuje integrację modeli z aplikacjami informatycznymi, projektowanie interfejsów użytkownika i interakcji z systemami AI, przetwarzanie danych tekstowych, ocenę jakości generowanych rezultatów oraz analizę ograniczeń i ryzyk związanych z wykorzystaniem technologii generatywnych. Omawiane są również zagadnienia odpowiedzialnego stosowania sztucznej inteligencji, ochrony danych, przejrzystości działania systemów oraz wpływu rozwiązań opartych na AI na użytkowników i organizacje. Kurs rozwija umiejętność łączenia metod inżynierii oprogramowania z technikami analizy języka naturalnego oraz skutecznej komunikacji technicznej w procesie tworzenia nowoczesnych aplikacji wspieranych przez sztuczną inteligencję.	K_W04, K_W07, K_W10 K_U04, K_U08, K_U09, K_U14 K_K03
Analiza wydajności i niezawodności systemów (semestr 3) W ramach kursu studenci zdobywają wiedzę i umiejętności związane z oceną wydajności, niezawodności oraz ograniczeń systemów informatycznych. Zakres obejmuje dobór i interpretację metryk jakościowych i ilościowych, projektowanie i realizację testów wydajnościowych, analizę wyników pomiarów, identyfikację wąskich gardeł oraz ocenę wpływu architektury systemu na jego efektywność, dostępność i niezawodność. Omawiane są również metody monitorowania pracy systemów, oceny ich odporności na obciążenia i awarie oraz formułowania rekomendacji dotyczących optymalizacji. Kurs rozwija umiejętność podejmowania decyzji technicznych w oparciu o dane pomiarowe, kryteria jakościowe oraz wymagania użytkowników i organizacji.	K_W02, K_W07, K_W08 K_U08, K_U10 K_U14 K_K03
MODUŁ PRAKTYKI	**EFEKTY KIERUNKOWE**
Praktyki zawodowe (semestr 1-2) W ramach praktyki zawodowej studenci pogłębiają doświadczenie zawodowe poprzez realizację specjalistycznych zadań w środowisku związanym z informatyką lub cyberbezpieczeństwem. Zakres praktyki obejmuje udział w pracach projektowych, administracyjnych, analitycznych, testowych lub związanych z zapewnianiem bezpieczeństwa systemów informatycznych, zgodnie z profilem działalności instytucji przyjmującej. Studenci wykorzystują narzędzia i metody stosowane w praktyce zawodowej, dokumentują przebieg wykonywanych działań, analizują uzyskane rezultaty oraz odnoszą zdobyte doświadczenia do efektów uczenia się określonych w programie studiów. Praktyka rozwija samodzielność, odpowiedzialność zawodową, umiejętność pracy zespołowej oraz przygotowuje do efektywnego funkcjonowania na rynku pracy.	K_W01, K_W02 K_W04, K_W05, K_W06, K_W08 K_U01, K_U02 K_U04, K_U05 K_U06, K_U07 K_U09, K_U10 K_U11 K_U13, K_U14 K_K01, K_K02, K_K03

PLAN STUDIÓW – ZAŁĄCZNIK 3b

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: DRUGI
Forma: NIESTACJONARNE
Nabór: 2026-2027

Semestr 1

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	grupa przedmiotów[1]	godziny kontaktowe								forma zaliczenia	punkty ECTS	ECTS/ udział NA	ECTS/ bez udziału NA	ECTS/ kształtujące umiejętności praktyczne	kod dyscypliny
		W	zajęć w grupach					e-learning	razem						
			A	K	L	S	P								
MODUŁ OGÓLNOUCZELNIANY		**0**	**0**	**0**	**0**	**0**	**0**	**6**	**6**		**0**	**0**	**0**	**0**	
Szkolenie biblioteczne	A							2	2	z	0				
Szkolenie BHK	A							4	4	z	0				
MODUŁ KIERUNKOWY		**45**	**45**	**0**	**65**	**0**	**0**	**0**	**155**		**18**	**6,2**	**11,8**	**11,5**	
Kryptografia stosowana i ochrona danych	C	10	20						30	E	4	1,2	2,8	3	ITiT
Zaawansowane technologie zabezpieczania infrastruktury sieciowej	C	10			20				30	zo	3	1,2	1,8	2,5	ITiT
Steganografia i ochrona informacji ukrytej	C	10			20				30	E	3	1,2	1,8	2	ITiT
Bezpieczeństwo systemów serwerowych	C				25				25	zo	3	1,0	2	2	ITiT
Projektowanie i inżynieria systemów informatycznych	C	10	15						25	zo	3	1,0	2	1,5	ITiT
Czynnik ludzki, kultura bezpieczeństwa i komunikacja kryzysowa	F	5	10						15	z	2	0,6	1,4	0,5	H/S
MODUŁ KURSÓW OBIERALNYCH		**15**	**0**	**0**	**35**	**0**	**0**	**0**	**50**		**6**	**2,0**	**4,0**	**4**	
Reagowanie na incydenty i informatyka śledcza	E	10			15				25	zo	3	1	2	2	ITiT
Bezpieczeństwo applikacji i DevSecOps	E	5			20				25	zo	3	1	2	2	ITiT
Programowanie systemowe i współbieżne w Rust	E	10			15				25	zo	3	1	2	2	ITiT
Tworzenie nowoczesnych aplikacji internetowych i API	E	5			20				25	zo	3	1	2	2	ITiT
MODUŁ PRAKTYKI[2]		**0**	**0**	**0**	**0**	**0**	**160**	**0**	**160**		**5**	**0**	**0**	**5**	
Praktyka zawodowa	H						160		160	z	5			5	
		60	45	0	100	0	160	6	211	0	29	8,2	15,8	20,5	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: DRUGI
Forma: NIESTACJONARNE
Nabór: 2026-2027

Semestr 2

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	grupa przedmiotów[1]	godziny kontaktowe								forma zaliczenia	punkty ECTS	ECTS/ udział NA	ECTS/ bez udziału NA	ECTS/ kształtujące umiejętności praktyczne	kod dyscypliny
		W	zajęć w grupach					e-learning	razem						
			A	K	L	S	P								
MODUŁ OGÓLNOUCZELNIANY		**0**	**0**	**15**	**0**	**0**	**0**	**0**	**15**		**1**	**0,6**	**0,4**	**1**	
Język angielski dla potrzeb rynku pracy B2+	G			15					15	zo	1	0,6	0,4	1	J
MODUŁ KIERUNKOWY		**20**	**0**	**0**	**75**	**15**	**0**	**0**	**110**		**12**	**4,4**	**7,6**	**8,5**	
SOC i monitoring bezpieczeństwa	C	5			20				25	E	3	1,0	2,0	2	ITiT
Bezpieczeństwo chmury i środowisk rozproszonych (techn. Blockchain)	C	5			20				25	zo	3	1,0	2,0	2	ITiT
Audyt bezpieczeństwa i testy penetracyjne	C	5			20				25	E	3	1,0	2,0	2	ITiT
Realizacja i zarządzanie przedsięwzięciem inżynierskim	C	5			15				20	zo	2	0,8	1,2	1,5	ITiT
Seminarium dyplomowe 1	C					15			15	z	1	0,6	0,4	1	ITiT
MODUŁ KURSÓW OBIERALNYCH		**25**	**0**	**0**	**50**	**0**	**0**	**0**	**75**		**9**	**3,0**	**6,0**	**6**	
Zaawansowane metody optymalizacji systemów komputerowych	E	5			20				25	zo	3	1,0	2,0	2	ITiT
Sztuczna inteligencja i detekcja anomalii w cyberbezpieczeństwie	E	10			15				25	zo	3	1,0	2,0	2	ITiT
Threat intelligence and threat hunting	E	10			15				25	zo	3	1,0	2,0	2	ITiT
Zaawansowane metody uczenia maszynowego	E	10			15				25	zo	3	1,0	2,0	2	ITiT
Programowanie Internetu rzeczy i systemów wbudowanych	E	10			15				25	zo	3	1,0	2,0	2	ITiT
Wizualizacja danych i komunikacja wyników	E	10			15				25	zo	3	1,0	2,0	2	ITiT
MODUŁ PRAKTYKI[3]		**0**	**0**	**0**	**0**	**0**	**320**	**0**	**320**		**9**	**0,0**	**0,0**	**9**	
Praktyka zawodowa	H						320		320	zo	9			9	
		45	0	15	125	15	320	0	200		31	8	14	24,5	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: DRUGI
Forma: NIESTACJONARNE
Nabór: 2026-2027

Semestr 3

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	grupa przedmiotów[1]	godziny kontaktowe								forma zaliczenia	punkty ECTS	ECTS/ udział NA	ECTS/ bez udziału NA	ECTS/ kształtujące umiejętności praktyczne	kod dyscypliny
		W	zajęć w grupach					e-learning	razem						
			A	K	L	S	P								
MODUŁ KIERUNKOWY		**39**	**20**	**0**	**15**	**15**	**0**	**0**	**89**		**10**	**3,6**	**6,4**	**6,5**	
Prawo, normy i compliance w cyberbezpieczeństwie	F	9	15						24	zo	3	1,0	2,0	1	H/S
Cyberprzestrzeń i cyberprzestępczość	C	20	5		5				30	zo	4	1,2	2,8	3	ITiT
Metody badawcze w naukach inżynieryjno-technicznych	C	10			10				20	zo	2	0,8	1,2	1,5	ITiT
Seminarium dyplomowe 2	C					15			15	z	1	0,6	0,4	1	ITiT
MODUŁ KURSÓW OBIERALNYCH		**55**	**5**	**0**	**40**	**0**	**0**	**0**	**100**		**12**	**4**	**8**	**5**	
Zarządzanie ryzykiem, ISMS i ciągłość działania	E	10			15				25	zo	3	1	2	2	ITiT
Bezpieczeństwo infrastruktury krytycznej, OT i IoT	E	10			15				25	zo	3	1	2	2	ITiT
Metody inżynierskie i komercjalizacja w branży IT	E	10	5		10				25	zo	3	1	2	1	ITiT
Wykład monograficzny: zagrożenia i trendy w cyberbezpieczeństwie	E	25							25	zo	3	1	2	0	ITiT
Przetwarzanie języka naturalnego	E	10			15				25	zo	3	1	2	2	ITiT
Programowanie na GPU i obliczenia równoległe	E	5			20				25	zo	3	1	2	2	ITiT
Projektowanie aplikacji z wykorzystaniem dużych modeli językowych	E	10			15				25	zo	3	1	2	2	ITiT
Analiza wydajności i niezawodności systemów	E	10			15				25	zo	3	1	2	2	ITiT
MODUŁ DYPLOMOWY		**0**	**0**	**0**	**0**	**0**	**0**	**0**			**8**	**0**	**0**	**8**	
Praca dyplomowa											8			8	ITiT
		94	25	0	55	15	0	0	189		30	7,6	14,4	19,5	

1. Grupa przedmiotów (A-obligatoryjne, B-podstawowe, C-kierunkowe, D-specjalnościowe, E-obieralne, F-humanistyczno-społeczne, G-języki obce, H-praktyki)
2. Praktyki 4 tyg. (160h lekcyjnych = 120h zegarowych)
3. Praktyki 8 tyg. (320h lekcyjnych = 240h zegarowych)

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: DRUGI
Forma: NIESTACJONARNE
Nabór: 2026-2027

PODSTAWOWE INFORMACJE O PROGRAMIE KSZTAŁCENIA I KIERUNKU STUDIÓW	CYBERBEZPIECZEŃSTWO
Liczba semestrów	3
Łączna liczba godzin pracy studenta w planie studiów	600
Łączna liczba punktów ECTS konieczna do ukończenia studiów	90
Łączna liczba godzin przeznaczonych na praktyki zawodowe	480
Łączna liczba punktów ECTS przeznaczonych na praktyki zawodowe	14
Łączna liczba punktów ECTS przeznaczonych na pracę dyplomową	8
Procentowy udział w ramach zajęć w bezpośrednim udziale NA	34,9%
Łączna liczba punktów ECTS powiązanych z działalnością naukową	75
Łączna liczba punktów ECTS powiązanych z działalnością naukową w dyscyplinie ITiT	70
Łączna liczba punktów ECTS kształtujących umiejętności praktyczne	64,5
Łączna liczba punktów ECTS przyporządkowanych kursom z zakresu nauk human.-społ. (F)	5
Łączna liczba godzin zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	199
Łączna liczba punktów ECTS przyporządkowanych kursom do wyboru	27
Łączna liczba punktów ECTS - procentowy udział kursów do wyboru	30,0%
Łączna liczba godzin zajęć z języków obcych	15
Łączna liczba punktów ECTS przypisana zajęciom z języków obcych	1

uken
Uniwersytet Komisji
Edukacji Narodowej
w Krakowie

INSTYTUT BEZPIECZEŃSTWA I INFORMATYKI

ul. Podchorążych 2, 30-084 Kraków
www.ii.uken.krakow.pl

tel. 12 662 7845
e-mail: ii@uken.krakow.pl

UNIWERSYTET
KOMISJI EDUKACJI NARODOWEJ
W KRAKOWIE
Instytut Bezpieczeństwa i Informatyki
30-060 Kraków, ul. Ingardena 4
tel. 12 662 66 04, 12 662 78 45

Kraków, dn. 22.06.2026 r.

Uchwała nr 19/IBiI/26
Rady Instytutu Bezpieczeństwa i Informatyki
Uniwersytetu Komisji Edukacji Narodowej w Krakowie
z dnia 22 czerwca 2026 r.

Rada Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie podjęła uchwałę o utworzeniu nowego kierunku studiów: **Cyberbezpieczeństwo** studiów drugiego stopnia o profilu praktycznym rozpoczynających się od roku akademickiego 2026/2027.

DYREKTOR
Instytutu Bezpieczeństwa i Informatyki
prof. dr hab. Olga Wasiuta

UNIWERSYTET
KOMISJI EDUKACJI NARODOWEJ
W KRAKOWIE
Instytut Bezpieczeństwa i Informatyki
30-060 Kraków, ul. Ingardena 4
tel. 12 662 66 04, 12 662 78 45

Kraków 19.06.2026 r.

OPINIA nr 8/RJK/2026

Rady Jakości Kształcenia dla kierunku

INFORMATYKA i CYBERBEZPIECZEŃSTWO

dotyczy

programu i planu studiów

dla nowego kierunku studiów

CYBERBEZPIECZEŃSTWO

studia II stopnia – stacjonarne i niestacjonarne

cykl 2026/27

Instytutowa Rada Jakości Kształcenia pozytywnie opiniuje utworzenie kierunku studiów drugiego stopnia „CYBERBEZPIECZEŃSTWO" oraz pozytywnie opiniuje program i plan studiów dla tego kierunku, obowiązujące od naboru na rok akademicki 2026-27.

Szczegółowe wyniki głosowania nad akceptacją programów i planów:

Liczba uprawnionych do głosowania: 13
Liczba oddanych głosów: 10
Akceptuję: 10
Nie akceptuję: 0
Wstrzymuję się: 0

Z-CA DYREKTORA
Instytutu Bezpieczeństwa i Informatyki
dr Beata Krzaczek

samorząd studentów

Uniwersytetu Komisji Edukacji Narodowej w Krakowie

Kraków, 21.06.2026

Opinia Instytutowej Rady Samorządu Studentów 6-IRSS-26

Instytutu Bezpieczeństwa i Informatyki

Uniwersytetu Komisji Edukacji Narodowej w Krakowie

w sprawie programów i planów studiów dla kierunków Informatyka oraz Cyberbezpieczeństwo (studia II stopnia) realizowanych w formie stacjonarnej i niestacjonarnej.

Na podstawie dostarczonych źródeł Instytutowa Rada Samorządu Studentów Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie dokonała oceny programów i planów studiów dla kierunków Informatyka oraz Cyberbezpieczeństwo II stopnia (studia stacjonarne i niestacjonarne) dla cyklu kształcenia rozpoczynającego się od roku akademickiego 2026/2027 i wyraża pozytywną opinię na ich temat.

Małgorzata Kościelniak

Przewodnicząca Instytutowej Rady Samorządu Studentów

Instytutu Bezpieczeństwa i Informatyki

Podpis:

Małgorzata Kościelniak