PROGRAM STUDIÓW WYŻSZYCH ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM 2026/2027

SPIS TREŚCI

OGÓLNA CHARAKTERYSTYKA KIERUNKU STUDIÓW

Jednostka badawczo-dydaktyczna prowadząca kierunek:	INSTYTUT BEZPIECZEŃSTWA I INFORMATYKI
Nazwa kierunku:	CYBERBEZPIECZEŃSTWO
Poziom:	STUDIA I STOPNIA
Profil:	PRAKTYCZNY
Forma:	STACJONARNE
Liczba punktów ECTS wymaganych do ukończenia studiów:	210 ECTS
Tytuł zawodowy nadawany absolwentom:	INŻYNIER
Poziom Polskiej Ramy Kwalifikacji:	SZÓSTY (6)
Termin rozpoczęcia cyklu:	2026/2027, SEMESTR ZIMOWY
Czas trwania studiów (liczba semestrów):	7 SEMESTRÓW
Dziedzina/-y:	NAUKI INŻYNIERYJNO-TECHNICZNE, NAUKI SPOŁECZNE, NAUKI ŚCISŁE I PRZYRODNICZE
Dyscyplina wiodąca:	INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA: 80%
Pozostałe dyscypliny:	NAUKI O BEZPIECZEŃSTWIE:15%, MATEMATYKA: 5%
Kod ISCED:	0612 - PROJEKTOWANIE I ADMINISTROWANIE BAZ DANYCH I SIECI

PODSTAWOWE INFORMACJE O PROGRAMIE KSZTAŁCENIA I KIERUNKU STUDIÓW	CYBERBEZPIECZEŃSTWO
Liczba semestrów	7
Łączna liczba godzin pracy studenta w planie studiów	2271
Łączna liczba punktów ECTS konieczna do ukończenia studiów	210
Łączna liczba godzin przeznaczonych na praktyki zawodowe	960
Łączna liczba punktów ECTS przeznaczonych na praktyki zawodowe	30
Łączna liczba punktów ECTS przeznaczonych na pracę dyplomową	8
Procentowy udział w ramach zajęć w bezpośrednim udziale NA	50,9%
Łączna liczba punktów ECTS w ramach zajęć w bezpośrednim udziale NA	87,6
Łączna liczba punktów ECTS powiązanych z działalnością naukową	210
Łączna liczba punktów ECTS powiązanych z działalnością naukową w dyscyplinie ITiT	161
Łączna liczba punktów ECTS kształtujących umiejętności praktyczne	126
Łączna liczba punktów ECTS przyporządkowanych kursom z zakresu nauk human.-społ. (F)	8
Łączna liczba godzin zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	746
Łączna liczba punktów ECTS przyporządkowanych kursom do wyboru	63
Łączna liczba punktów ECTS - procentowy udział kursów do wyboru	30,0%
Łączna liczba godzin zajęć z wychowania fizycznego	60
Łączna liczba godzin zajęć z języków obcych	110
Łączna liczba punktów ECTS przypisana zajęciom z języków obcych	10

ZWIĄZEK Z MISJĄ UCZELNI I STRATEGIĄ JEJ ROZWOJU

Kierunek Cyberbezpieczeństwo, studia pierwszego 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 kompetencje praktyczne, analityczne i projektowe w zakresie bezpieczeństwa systemów teleinformatycznych, ochrony danych oraz przeciwdziałania cyberzagrożeniom, odpowiadające aktualnym 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. Jednocześnie kierunek realizuje założenia Obszaru II – Badania naukowe i rozwój dyscyplin, poprzez rozwijanie kompetencji badawczych studentów, włączanie ich w realizację projektów naukowych oraz kształtowanie umiejętności analizy zagrożeń, identyfikacji podatności systemów informatycznych oraz rozwiązywania złożonych problemów związanych z bezpieczeństwem cyberprzestrzeni. 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 informacji i bezpieczeństwa cyfrowego. Profil praktyczny studiów stanowi odpowiedź na wyzwania związane z transformacją cyfrową, dynamicznym rozwojem technologii informacyjno-komunikacyjnych oraz rosnącą skalą zagrożeń cybernetycznych. Program studiów uwzględnia aktualne potrzeby rynku pracy w zakresie bezpieczeństwa sieci komputerowych, ochrony danych, bezpieczeństwa systemów operacyjnych i aplikacji oraz zarządzania bezpieczeństwem informacji, wzmacniając tym samym pozycję absolwentów na rynku pracy.

WARUNKI REKRUTACJI

Kandydaci z „nową maturą": podstawą kwalifikacji kandydatów jest postępowanie rankingowe. Wynik kandydata wyrażony w punktach ustala się jako większą z wartości:

- liczba punktów uzyskanych z egzaminu maturalnego z matematyki - poziom podstawowy, część pisemna,
- dwukrotność liczby punktów uzyskanych z egzaminu maturalnego z matematyki lub informatyki - poziom rozszerzony, część pisemna.

Przyjmuje się zasadę: 1% = 1 punkt.

Kandydaci ze „starą maturą": podstawą kwalifikacji kandydatów jest postępowanie rankingowe. Wynik kandydata ustala się jako większą z wartości:

- liczba punktów odpowiadająca ocenie z pisemnego egzaminu dojrzałości z matematyki lub informatyki,
- liczba punktów odpowiadająca ocenie z ustnego egzaminu dojrzałości z matematyki lub informatyki,
- 0,75 wartości punktowej odpowiadającej ocenie z egzaminu dojrzałości (część pisemna) z jednego z przedmiotów: fizyka lub chemia.

Przelicznik ocen (stara matura) - oceny ze świadectwa dojrzałości przelicza się na punkty według następującej skali:

- dopuszczający - 30 punktów
- dostateczny - 50 punktów
- dobry - 70 punktów
- bardzo dobry - 90 punktów
- celujący - 100 punktów

Laureaci i finaliści olimpiad: laureaci oraz finaliści olimpiad stopnia centralnego są przyjmowani na studia zgodnie z zasadami określonymi w aktualnej uchwale Senatu Uniwersytetu Komisji Edukacji Narodowej w Krakowie obowiązującej w roku rekrutacji. Organizacja procesu kształcenia na kierunku odbywa się zgodnie z programem studiów obowiązującym dla danego cyklu kształcenia. Studenci realizują moduły obowiązkowe oraz kursy obieralne zgodnie z zasadami określonymi w programie studiów i harmonogramie organizacji roku akademickiego. Wyboru kursów obieralnych studenci dokonują w terminach określonych przez uczelnię, z uwzględnieniem liczby dostępnych miejsc oraz zasad organizacji zajęć dydaktycznych. Uruchomienie poszczególnych kursów obieralnych może być uzależnione od liczby studentów deklarujących udział w danych zajęciach.

SYLWETKA ABSOLWENTA

Absolwent kierunku Cyberbezpieczeństwo, studiów pierwszego stopnia o profilu praktycznym, posiada interdyscyplinarną wiedzę z zakresu nauk inżynieryjno-technicznych, informatycznych, ścisłych oraz społecznych, niezbędną do projektowania, wdrażania i utrzymania bezpiecznych systemów teleinformatycznych. Jest przygotowany do funkcjonowania w dynamicznie zmieniającym się środowisku cyfrowym oraz rozumie znaczenie bezpieczeństwa informacji dla funkcjonowania administracji publicznej, przedsiębiorstw i społeczeństwa informacyjnego. Absolwent dysponuje wiedzą w zakresie: bezpieczeństwa systemów operacyjnych, aplikacji oraz sieci komputerowych, projektowania, konfiguracji i administrowania infrastrukturą teleinformatyczną z uwzględnieniem zasad cyberbezpieczeństwa, metod wykrywania, analizy i przeciwdziałania cyberzagrożeniom, ochrony danych, bezpieczeństwa informacji oraz zarządzania dostępem do zasobów cyfrowych, kryptografii, uwierzytelniania oraz mechanizmów zapewniania poufności, integralności i dostępności danych, bezpieczeństwa usług internetowych, aplikacji mobilnych oraz systemów chmurowych, wykorzystania nowoczesnych technologii, w tym elementów sztucznej inteligencji i automatyzacji procesów bezpieczeństwa, uwarunkowań prawnych, organizacyjnych i etycznych związanych z cyberbezpieczeństwem oraz ochroną danych osobowych. Absolwent zna współczesne zagrożenia występujące w cyberprzestrzeni, w szczególności: cyberprzestępczość i techniki prowadzenia cyberataków, zagrożenia dla bezpieczeństwa informacji i ciągłości działania systemów, zagrożenia związane z funkcjonowaniem użytkowników w środowisku cyfrowym, w tym cyberprzemoc, dezinformację i wybrane patologie cyfrowe, ryzyka wynikające z rozwoju nowoczesnych technologii informacyjno-komunikacyjnych. Absolwent posiada umiejętności i kompetencje umożliwiające: projektowanie, wdrażanie i utrzymywanie bezpiecznych systemów oraz sieci teleinformatycznych, konfigurację i administrację systemami operacyjnymi, usługami sieciowymi oraz urządzeniami infrastruktury teleinformatycznej, identyfikację podatności, analizę incydentów bezpieczeństwa oraz reagowanie na cyberzagrożenia, stosowanie narzędzi wspierających monitorowanie bezpieczeństwa i ochronę infrastruktury cyfrowej, wykorzystanie środowisk programistycznych oraz podstaw automatyzacji w realizacji zadań związanych z cyberbezpieczeństwem, pracę indywidualną i zespołową przy realizacji projektów technicznych, komunikowanie zagadnień związanych z bezpieczeństwem informacji w sposób zrozumiały dla użytkowników i organizacji, przestrzeganie zasad etyki zawodowej oraz odpowiedzialne wykonywanie obowiązków związanych z ochroną danych i bezpieczeństwem cyfrowym. Absolwent jest przygotowany do podjęcia pracy m.in. w działach bezpieczeństwa IT, centrach monitorowania bezpieczeństwa (SOC), zespołach administracji systemami i sieciami komputerowymi, firmach technologicznych, instytucjach publicznych oraz podmiotach odpowiedzialnych za ochronę infrastruktury informacyjnej. Jest również przygotowany do dalszego rozwoju zawodowego i kontynuowania kształcenia na studiach drugiego stopnia.

UZYSKIWANE KWALIFIKACJE ORAZ UPRAWNIENIA ZAWODOWE

Absolwent kierunku Cyberbezpieczeństwo studiów pierwszego stopnia o profilu praktycznym uzyskuje kwalifikacje umożliwiające podjęcie pracy zawodowej zarówno w sektorze publicznym, jak i prywatnym, w obszarach związanych z bezpieczeństwem systemów teleinformatycznych, ochroną danych oraz przeciwdziałaniem cyberzagrożeniom. Mogą znaleźć zatrudnienie w podmiotach odpowiedzialnych za zapewnienie bezpieczeństwa cyberprzestrzeni, w tym w instytucjach tworzących krajowy system cyberbezpieczeństwa, służbach odpowiedzialnych za zwalczanie cyberprzestępczości, jednostkach zajmujących się ochroną infrastruktury krytycznej oraz organizacjach realizujących zadania z zakresu bezpieczeństwa informacji. Absolwenci są przygotowani do pracy m.in. na stanowiskach: administratora sieci i systemów komputerowych, specjalisty ds. cyberbezpieczeństwa, analityka bezpieczeństwa, konsultanta ds. bezpieczeństwa informacji, inżyniera bezpieczeństwa systemów teleinformatycznych, pentestera i specjalisty ds. testów bezpieczeństwa, programisty tworzącego bezpieczne aplikacje i rozwiązania informatyczne, specjalisty ds. monitorowania i reagowania na incydenty bezpieczeństwa. Kompetencje zdobyte podczas studiów umożliwiają również podjęcie pracy w administracji publicznej, instytucjach edukacyjnych oraz organizacjach społecznych i eksperckich zajmujących się bezpieczeństwem cyfrowym, ochroną informacji, przeciwdziałaniem dezinformacji oraz rozwijaniem kompetencji cyfrowych społeczeństwa. Absolwent jest również przygotowany do dalszego rozwoju zawodowego, uzyskiwania certyfikacji branżowych oraz kontynuowania kształcenia na studiach drugiego stopnia.

PRAKTYKI ZAWODOWE

W programie studiów na kierunku Cyberbezpieczeństwo (studia pierwszego stopnia) przewidziano obowiązkowe praktyki zawodowe, realizowane w celu osiągnięcia efektów uczenia się związanych z praktycznym przygotowaniem do wykonywania zadań zawodowych w obszarze bezpieczeństwa systemów teleinformatycznych oraz ochrony informacji. Praktyki zawodowe realizowane są w łącznym wymiarze 960 godzin lekcyjnych (720 godzin zegarowych). W przypadku studiów stacjonarnych praktyki realizowane są w semestrze VI, natomiast w przypadku studiów niestacjonarnych w semestrach V–VII, po 320 godzin w każdym semestrze. Przyjęty wymiar godzinowy praktyk wynika ze specyfiki kierunku oraz konieczności osiągnięcia zakładanych efektów uczenia się. Za realizację praktyk zawodowych student uzyskuje 30 punktów ECTS. Student realizuje zadania zawodowe w rzeczywistym środowisku pracy, uczestnicząc w działaniach związanych z bezpieczeństwem systemów i sieci komputerowych, ochroną danych, monitorowaniem incydentów bezpieczeństwa, administracją systemami teleinformatycznymi oraz analizą zagrożeń cybernetycznych 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 w obszarze cyberbezpieczeństwa, bezpieczeństwa informacji, administracji systemów i sieci komputerowych, ochrony danych, usług IT oraz monitorowania i reagowania na incydenty bezpieczeństwa, w szczególności w działach bezpieczeństwa IT przedsiębiorstw i instytucji, centrach monitorowania bezpieczeństwa (SOC), firmach świadczących usługi z zakresu cyberbezpieczeństwa, jednostkach administracji publicznej odpowiedzialnych za bezpieczeństwo informacji, podmiotach zajmujących się utrzymaniem infrastruktury teleinformatycznej, organizacjach realizujących zadania związane z ochroną danych i bezpieczeństwem cyfrowym.

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 kluczowe zagadnienia z zakresu informatyki, matematyki, logiki, algorytmiki, struktur danych i podstaw kodowania, niezbędne do analizy problemów cyberbezpieczeństwa.	P6U_W P6S_WG
K_W02	Absolwent zna i rozumie architekturę komputerów, systemów operacyjnych, sieci komputerowych, baz danych, systemów chmurowych oraz środowisk rozproszonych w kontekście ich konfiguracji, administracji i zabezpieczania.	P6U_W P6S_WG inż_P6S_WG
K_W03	Absolwent zna i rozumie w zaawansowanym stopniu współczesne zagrożenia, podatności, modele ataków oraz techniki ochrony systemów, sieci komputerowych, aplikacji internetowych, baz danych i usług cyfrowych.	P6U_W P6S_WG
K_W04	Absolwent zna i rozumie w zaawansowanym stopniu mechanizmy kryptografii, ochrony informacji, kontroli dostępu, uwierzytelniania, autoryzacji oraz bezpiecznego przetwarzania danych w systemach teleinformatycznych.	P6U_W P6S_WG
K_W05	Absolwent zna i rozumie w zaawansowanym stopniu zasady projektowania, implementacji, testowania i utrzymania oprogramowania wykorzystywanego w cyberbezpieczeństwie, w tym oprogramowania skryptowego, systemowego, niskopoziomowego oraz aplikacji internetowych, z uwzględnieniem zasad bezpiecznego programowania.	P6U_W P6S_WG inż_P6S_WG
K_W06	Absolwent zna i rozumie ekonomiczne, prawne, etyczne, społeczne i organizacyjne uwarunkowania działalności inżynierskiej w obszarze cyberbezpieczeństwa, w tym metody zarządzania ryzykiem, standardy i normy bezpieczeństwa, regulacje dotyczące ochrony informacji i własności intelektualnej, a także aspekty przedsiębiorczości i bezpieczeństwa państwa.	P6U_W P6S_WK
K_W07	Absolwent zna i rozumie w zaawansowanym stopniu procesy monitorowania bezpieczeństwa, wykrywania cyberataków, reagowania na incydenty, analizy śladów cyfrowych, informatyki śledczej oraz podstawy inżynierii odwrotnej.	P6U_W P6S_WG
K_W08	Absolwent zna i rozumie w zaawansowanym stopniu założenia sztucznej inteligencji, uczenia maszynowego, systemów dużych modeli językowych oraz ich zastosowania w cyberbezpieczeństwie, w tym podatności i metody zabezpieczania takich systemów.	P6U_W P6S_WG
K_W09	Absolwent zna i rozumie technologie DevSecOps, systemy kontroli wersji oraz procesy integracji, testowania i wdrażania bezpiecznego oprogramowania.	P6U_W P6S_WG inż_P6S_WG
K_W10	Absolwent zna i rozumie technologie decentralizacji danych, w tym blockchain, a także wybrane zagadnienia bezpieczeństwa systemów elektronicznych, przetwarzania sygnałów oraz technologii chmurowych.	P6U_W P6S_WG
K_W11	Absolwent zna i rozumie społeczne, strategiczne i militarne uwarunkowania cyberbezpieczeństwa, w tym zjawiska dezinformacji, wojny informacyjnej oraz zarządzania kryzysowego.	P6U_W P6S_WG
K_W12	Absolwent zna i rozumie zasady, metodyki i narzędzia związane z cyklem życia systemów cyberbezpieczeństwa, zarządzaniem projektami w obszarze bezpieczeństwa teleinformatycznego, zapewnianiem jakości, bezpieczeństwa i niezawodności systemów oraz stosowaniem dobrych praktyk inżynierskich.	P6U_W P6S_WG P6S_WK inż_P6S_WG
K_W13	Absolwent zna i rozumie podstawową terminologię obcojęzyczną właściwą dla informatyki oraz rozumie rolę języka obcego w dostępie do dokumentacji, źródeł wiedzy i komunikacji zawodowej.	P6U_W P6S_WG P6S_WK
K_W14	Absolwent zna i rozumie zasady odpowiedzialnego i zgodnego z obowiązującymi regulacjami korzystania z zasobów uczelni, w tym w zakresie bezpieczeństwa i higieny pracy oraz dostępu do źródeł informacji naukowej.	P6U_W P6S_WK

	UMIEJĘTNOŚCI	
K_U01	Absolwent potrafi stosować wiedzę matematyczną, logiczną i algorytmiczną do modelowania, analizowania i rozwiązywania problemów informatycznych oraz problemów cyberbezpieczeństwa.	P6U_U P6S_UW
K_U02	Absolwent projektuje, implementuje, testuje i dokumentuje programy komputerowe z wykorzystaniem różnych paradygmatów i języków programowania, w tym Python, C/C++, Java oraz języków skryptowych.	P6U_U P6S_UW inż_P6S_UW
K_U03	Absolwent konfiguruje, administruje i zabezpiecza systemy operacyjne, usługi sieciowe, bazy danych, aplikacje internetowe oraz podstawowe środowiska chmurowe.	P6U_U P6S_UW
K_U04	Absolwent dokonuje analizy architektury systemów komputerowych i sieciowych, identyfikuje ich podatności oraz dobiera adekwatne mechanizmy ochrony.	P6U_U P6S_UW inż_P6S_UW
K_U05	Absolwent stosuje narzędzia kryptograficzne, mechanizmy kontroli dostępu, uwierzytelniania i autoryzacji do ochrony danych oraz usług cyfrowych.	P6U_U P6S_UW
K_U06	Absolwent przeprowadza testy bezpieczeństwa, testy penetracyjne, analizę podatności oraz ocenę ryzyka technicznego i organizacyjnego.	P6U_U P6S_UW
K_U07	Absolwent monitoruje zdarzenia bezpieczeństwa, analizuje logi, wykrywa symptomy cyberataków oraz proponuje działania zapobiegawcze i naprawcze.	P6U_U P6S_UW
K_U08	Absolwent wykonuje analizę malware, analizę kodu, inżynierię odwrotną oraz analizę śladów cyfrowych zgodnie z zasadami informatyki śledczej.	P6U_U P6S_UW
K_U09	Absolwent wykorzystuje metody sztucznej inteligencji i uczenia maszynowego do wspomagania detekcji anomalii, reagowania na incydenty i analizy danych w cyberbezpieczeństwie.	P6U_U P6S_UW
K_U10	Absolwent ocenia bezpieczeństwo systemów sztucznej inteligencji i dużych modeli językowych oraz dobiera metody ograniczania ryzyk związanych z ich użyciem.	P6U_U P6S_UW
K_U11	Absolwent potrafi wykorzystywać repozytoria kodu, narzędzia kontroli wersji oraz potoki DevSecOps do integracji, testowania i wdrażania bezpiecznego oprogramowania.	P6U_U P6S_UW inż_P6S_UW
K_U12	Absolwent potrafi wykorzystywać uwarunkowania prawne, ekonomiczne i organizacyjne w planowaniu oraz realizacji działań związanych z projektowaniem, wdrażaniem i rozwojem systemów oraz rozwiązań z zakresu cyberbezpieczeństwa, z uwzględnieniem zasad ochrony własności intelektualnej i przedsiębiorczości.	P6U_U P6S_UW P6S_UO
K_U13	Absolwent potrafi opracowywać dokumentację techniczną, raporty z analiz bezpieczeństwa i testów, komunikować się z otoczeniem zawodowym z wykorzystaniem specjalistycznej terminologii z zakresu cyberbezpieczeństwa oraz prezentować wyniki prac w języku polskim i obcym właściwym dla środowiska zawodowego.	P6U_U P6S_UW P6S_UK
K_U14	Absolwent potrafi planować i realizować zadania zawodowe oraz projektowe w środowisku praktycznym, współdziałać z innymi osobami w ramach realizowanych działań, integrować wiedzę z różnych obszarów cyberbezpieczeństwa oraz przygotowywać projekty inżynierskie.	P6U_U P6S_UW P6S_UO inż_P6S_UW
K_U15	Absolwent potrafi samodzielnie rozwijać swoje kompetencje, korzystać z różnorodnych źródeł wiedzy i doświadczeń zawodowych oraz planować i realizować własne uczenie się przez całe życie w celu rozwiązywania praktycznych problemów inżynierskich.	P6U_U P6S_UU
K_U16	Absolwent potrafi stosować zasady bezpieczeństwa i higieny pracy podczas korzystania z zasobów uczelni oraz efektywnie wyszukiwać i wykorzystywać informacje z literatury naukowej, dokumentacji technicznej i zasobów bibliotecznych.	P6U_U P6S_UW P6S_UU
	KOMPETENCJE	
K_K01	Absolwent jest gotów do krytycznej oceny posiadanej wiedzy, uznawania znaczenia wiedzy eksperckiej oraz ciągłego uczenia się i aktualizowania kompetencji zawodowych w tym kompetencji językowych oraz korzystania z wiarygodnych źródeł informacji naukowej.	P6U_K P6S_KK

K_K02	Absolwent jest gotów do odpowiedzialnego pełnienia ról zawodowych w obszarze cyberbezpieczeństwa i informatyki, przestrzegania zasad etyki, ochrony informacji i własności intelektualnej oraz dbałości o jakość, bezpieczeństwo i rzetelność realizowanych zadań, w tym stosowania zasad bezpieczeństwa i higieny pracy.	P6U_K P6S_KO P6S_KR
K_K03	Absolwent jest gotów do współpracy w zespole, respektowania zasad komunikacji i organizacji pracy oraz podejmowania odpowiedzialności za realizację wspólnych zadań.	P6U_K P6S_KO
K_K04	Absolwent jest gotów do myślenia i działania w sposób przedsiębiorczy oraz do uwzględniania społecznych, ekonomicznych, organizacyjnych i prawnych skutków działań związanych z cyberbezpieczeństwem i systemami informatycznymi.	P6U_K P6S_KO P6S_KR

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_W12	K_W13	K_W14
K_U01	X		X											
K_U02	X				X				X					
K_U03		X	X	X						X				
K_U04		X	X	X						X		X		
K_U05			X	X	X									
K_U06			X			X	X			X		X		
K_U07			X				X					X		
K_U08			X		X		X							
K_U09	X						X	X						
K_U10			X			X		X						
K_U11					X				X			X		
K_U12						X					X	X		X
K_U13							X					X	X	X
K_U14					X	X					X	X		
K_U15													X	X
K_U16						X							X	X

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_W12	K_W13	K_W14	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_U15	K_U16	K_K01	K_K02	K_K03	K_K04
Szkolenie BHK	1														1																1		1		
Szkolenie biblioteczne	1														1																1	1			
Ochr. własności intelektualnej	1						1								1											1				1		1		
Wykład z zakresu nauk hum.-społ.	1						1					1															1		1		1		1	1
Podst. przedsiębiorcz.	1						1																			1		1						1
Wstęp do matematyki	1	1														1															1			
Matematyka dyskretna	1	1														1															1			
Teoret. podst. informatyki	1	1														1			1												1			
Programowanie	1	1				1											1															1		
Wstęp do cyberbezp.	1			1			1	1				1							1								1				1			
Teoria bezpieczeństwa	1						1					1															1							1
Języki skryptowe	1					1											1								1							1		
Progr. funkcyjne (Python)	1					1											1															1		
Język obcy B2 - 1	2													1													1		1		1			
Matematyka 1	2	1														1															1			
Organ. i arch. komp.	2		1															1	1												1		1	
Algorytmy i struktury danych	2	1				1										1	1														1			
Wprowadz. do sieci komp.	2		1	1														1	1													1		
Programowanie obiektowe	2					1											1															1		
Podst. syst. kontroli wersji i pracy zesp. w IT	2									1			1												1			1				1	1	
Progr. syst. (C lub C++)	2		1			1											1	1														1		
J. hipertekst. i tw. stron WWW	2			1		1											1	1														1		
Język obcy B2 - 1	3													1													1		1		1			
Matematyka 2	3	1														1															1			
Podstawy kodowania	3	1			1											1				1											1		1	
Systemy operacyjne	3		1	1														1	1													1		
Konfig. i zarz. sieciami komp.	3		1	1														1	1			1										1		
Wprowadzenie do techn. chmury	3		1								1							1	1													1		
Standaryzacja syst. cyberbezp.	3						1						1								1						1	1				1		
Technologie DevSecOps	3									1			1													1		1	1			1	1	
Programowanie niskopoziomowe	3		1			1											1	1														1		
Progr. aplikacji intern. (Java)	3			1		1											1	1														1		
Język obcy B2 - 1	4													1													1		1		1			
Fizyka i elektronika	4	1									1					1			1												1	1	1	
Podst. sztucznej inteligencji	4	1							1															1	1						1			
Bazy danych	4		1	1														1	1												1		1	
Bezp. systemów operacyjnych	4		1	1				1										1	1			1										1		
Bezp. sieci komputerowych	4		1	1	1			1										1	1		1	1										1		
Militarny wymiar cyberbezp.	4						1					1															1	1						1
Teoria zarz. ryz. cyberbezp.	4						1						1								1						1		1					1
Przetwarzanie sygnałów	4	1									1					1			1												1		1	
Bezp. technologii chmurowych	4		1	1							1							1	1		1											1		

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_W12	K_W13	K_W14	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_U15	K_U16	K_K01	K_K02	K_K03	K_K04
Bezpieczeństwo baz danych	5		1	1	1													1	1	1												1		
Kryptografia	5	1			1											1				1												1			
Bezp. aplikacji internetowych	5			1	1	1												1	1	1	1												1		
Inżynieria odwrotna	5					1		1													1		1										1		
Zarz. projektami cyberbezp.	5						1						1														1	1	1					1	1
Metody zbierania informacji	5			1				1														1	1					1					1		
Wojny informacyjne	5						1					1															1	1							1
Podst. prawne cyberbezp.	5						1																				1	1					1		1
Metody i narz. zabezp. aplik. AI	5			1					1												1				1								1		
Bezp. systemów AI i LLM	5			1					1															1	1								1		
Bezp. systemów elektronicznych	5		1	1							1								1		1												1		
AI w reagow. na inc. w krym. cyfr.	5							1	1													1	1	1									1		
Praktyka: BSiST	6	1	1	1				1		1			1			1		1	1							1			1	1		1	1	1	1
Praktyka: BAiD	6	1	1			1				1			1			1	1	1								1			1	1		1	1	1	1
Techn. decentr. danych (Blockchain)	7														1															1	1			
Techn. wykryw. I zap. cyberatakom	7						1								1												1				1		1		
Metodyki testów penetracyjnych	7						1					1																1		1		1		1	1
Projekt inżynierski	7						1																				1		1						1
Deepfake i bezp. poznawcze	7	1														1																1		1	
Zarządzanie kryzysowe	7	1														1																1		1	
Zarz. strateg. W cyberbezp.	7	1														1			1														1		1	
		K_W01	K_W02	K_W03	K_W04	K_W05	K_W06	K_W07	K_W08	K_W09	K_W10	K_W11	K_W12	K_W13	K_W14	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_U15	K_U16	K_K01	K_K02	K_K03	K_K04
Liczba przypisań do przedmiotów		17	15	17	5	12	14	7	4	4	5	6	7	3	5	15	10	17	18	4	8	5	3	3	3	5	12	12	8	7	5	27	32	15	12

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 realizowane w środowiskach laboratoryjnych, konfiguracja systemów i sieci komputerowych, analiza incydentów bezpieczeństwa, sprawozdania, prezentacje oraz aktywność 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 i projektów. 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, organizacji pracy oraz stosowania zasad bezpieczeństwa informacji i odpowiedzialności zawodowej. Na poziomie całego cyklu kształcenia osiągnięcie efektów uczenia się potwierdzane jest poprzez zaliczenie wszystkich etapów studiów, realizację praktyk zawodowych oraz przygotowanie i prezentację zespołowego projektu inżynierskiego stanowiącego rozwiązanie problemu praktycznego z zakresu cyberbezpieczeństwa lub bezpieczeństwa systemów teleinformatycznych, a także zdanie egzaminu inżynierskiego obejmującego część projektową (obrona projektu) oraz część pisemną. 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 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_W14 K_U16 K_K02
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_W14 K_U16 K_K01
Ochrona własności intelektualnej (semestr 1): Treści kształcenia obejmują zagadnienia związane z ochroną własności intelektualnej w kontekście funkcjonowania gospodarki cyfrowej. W ramach zajęć omawiane są podstawy prawne ochrony praw autorskich oraz własności przemysłowej, w tym zasady ochrony programów komputerowych, baz danych, znaków towarowych i patentów. Poruszane są również kwestie licencjonowania, przenoszenia praw oraz dozwolonego użytku. Szczególną uwagę poświęca się zastosowaniom przepisów w działalności informatycznej, a także problematyce naruszeń praw własności intelektualnej i związanej z nimi odpowiedzialności. Uzupełnieniem treści są praktyczne aspekty korzystania z zasobów cyfrowych oraz zawierania umów w obszarze IT.	K_W06, K_W14 K_U12, K_U16 K_K02
Wykład z zakresu nauk humanistyczno-społecznych (semestr 1): W ramach zajęć studenci zapoznają się z wybranymi zagadnieniami z zakresu nauk humanistycznych lub społecznych, rozwijając umiejętności analizy zjawisk kulturowych, społecznych i historycznych. Kurs umożliwia zrozumienie kontekstu omawianych problemów, ich przyczyn i skutków, a także poznanie metod badawczych stosowanych w naukach humanistycznych i społecznych. Tematyka wykładu może obejmować różne obszary, w tym kwestie polityczne, społeczne, ekonomiczne czy kulturowe, przy czym każdorazowo uwzględniane są aktualne konteksty, uwarunkowania historyczne i perspektywy rozwoju omawianych zagadnień.	K_W06, K_W11 K_U13, K_U15 K_K01, K_K03, K_K04
Podstawy przedsiębiorczości (semestr 1): W ramach zajęć studenci zapoznają się z podstawową wiedzą z zakresu przedsiębiorczości, obejmującą kluczowe pojęcia ekonomiczne, modele biznesowe oraz proces uruchamiania i prowadzenia firmy, ze szczególnym uwzględnieniem specyfiki branży informatycznej. Kurs rozwija umiejętności rozpoznawania szans rynkowych, formułowania celów biznesowych, analizowania podstawowych zagadnień prawnych oraz przygotowywania prostych biznesplanów i strategii rozwoju przedsiębiorstwa informatycznego. Studenci zdobywają praktyczne kompetencje pozwalające na samodzielne planowanie i podejmowanie decyzji w kontekście prowadzenia działalności gospodarczej.	K_W06 K_U12, K_U14 K_K04
Język obcy B2 - 1 (semestr 2): W ramach zajęć rozwijane są kompetencje językowe studentów w zakresie rozumienia tekstu słuchanego i czytanego, mówienia oraz pisania na poziomie B2 zgodnie z wymaganiami ESOKJ. Studenci doskonalą umiejętność komunikowania się w sytuacjach życia codziennego oraz akademickiego, formułowania spójnych wypowiedzi, wyrażania opinii oraz opisywania doświadczeń i planów. Wprowadzane jest również podstawowe słownictwo związane z obszarem informatyki oraz pracy w środowisku technologicznym.	K_W13 K_U13, K_U15 K_K01

Język obcy B2 - 2 (semestr 3): W ramach zajęć rozwijane są kompetencje językowe na poziomie B2 ze szczególnym uwzględnieniem komunikacji akademickiej i zawodowej w obszarze informatyki. Studenci doskonalą umiejętność prowadzenia dyskusji, prezentowania informacji oraz rozumienia bardziej złożonych tekstów i materiałów technicznych. Wprowadzane i utrwalane jest słownictwo specjalistyczne związane z technologiami informatycznymi, pracą zespołową oraz komunikacją w środowisku zawodowym.	K_W13 K_U13, K_U15 K_K01
Język obcy B2 - 3 (semestr 4): W ramach zajęć utrwalane i rozwijane są kompetencje językowe na poziomie B2 w kontekście akademickim i zawodowym związanym z informatyką. Studenci doskonalą umiejętność interpretowania tekstów specjalistycznych, przygotowywania prezentacji oraz formułowania wypowiedzi ustnych i pisemnych dotyczących zagadnień technicznych. Zajęcia obejmują również rozwijanie umiejętności korzystania z obcojęzycznych materiałów branżowych oraz komunikacji w środowisku zawodowym IT.	K_W13 K_U13, K_U15 K_K01
MODUŁ PODSTAWOWY	**EFEKTY KIERUNKOWE**
Wstęp do matematyki (semestr 1): W ramach zajęć studenci wyrównują poziom wiedzy matematycznej poprzez powtórzenie i utrwalenie zagadnień ze szkoły średniej, niezbędnych do dalszego kształcenia na kierunku Cyberbezpieczeństwo. Omawiane są podstawowe pojęcia z zakresu algebry, funkcji, równań i nierówności, elementów algebry wektorów oraz trygonometrii. Zajęcia mają na celu rozwijanie umiejętności logicznego myślenia i rozwiązywania problemów matematycznych, przygotowując studentów do kolejnych kursów matematycznych i informatycznych.	K_W01 K_U01 K_K01
Matematyka dyskretna (semestr 1): W ramach zajęć studenci zapoznają się z podstawowymi zagadnieniami matematyki dyskretnej i ich zastosowaniami w informatyce, w szczególności z logiką matematyczną, algebrą Boole'a, teorią zbiorów i relacji, indukcją matematyczną, kombinatoryką, teorią grafów oraz elementami rachunku prawdopodobieństwa i zmiennych losowych. Zajęcia rozwijają umiejętności logicznego myślenia, modelowania i analizy problemów oraz stosowania narzędzi matematyki dyskretnej w informatyce i cyberbezpieczeństwie, w szczególności w zakresie analizy algorytmów, kryptografii oraz bezpieczeństwa informacji.	K_W01 K_U01 K_K01
Teoretyczne podstawy informatyki (semestr 1): W ramach zajęć studenci zapoznają się z fundamentalnymi koncepcjami teoretycznej informatyki oraz ich praktycznymi zastosowaniami. Kurs obejmuje zagadnienia związane z systemami liczbowymi i ich reprezentacją w pamięci komputera, podstawowymi cechami i własnościami algorytmów oraz strukturami danych. Studenci poznają języki formalne, wyrażenia regularne, automaty skończone oraz gramatyki bezkontekstowe, a także elementy teorii obliczalności i podstaw teorii informacji. Zajęcia rozwijają umiejętności analitycznego i logicznego myślenia oraz przygotowują do samodzielnego pogłębiania wiedzy w zakresie informatyki, a także do zrozumienia teoretycznych podstaw dalszych zagadnień informatycznych, w tym projektowania i weryfikacji systemów komputerowych.	K_W01 K_U01, K_U04 K_K01
Programowanie (semestr 1): W ramach zajęć studenci zapoznają się z podstawami programowania imperatywnego o cechach strukturalnych i proceduralnych. Kurs obejmuje tworzenie prostych programów, podstawy algorytmiki, pisanie kodu, debugowanie i testowanie. Studenci rozwijają umiejętności logicznego myślenia, rozwiązywania problemów oraz strukturalnego podejścia do programowania, przygotowując się do bardziej zaawansowanych kursów w zakresie tworzenia oprogramowania i algorytmów.	K_W01, K_W05 K_U02 K_K02

Wstęp do cyberbezpieczeństwa (semestr 1): W ramach zajęć studenci zapoznają się z podstawowymi pojęciami, zasadami i praktykami cyberbezpieczeństwa oraz bezpieczeństwa informacji. Kurs obejmuje zagadnienia dotyczące cyberprzestrzeni, rodzajów cyberataków, podatności, ryzyka oraz podstawowych mechanizmów ochrony informacji, w tym identyfikacji, uwierzytelniania, autoryzacji i kontroli dostępu. Omawiane są również zagrożenia wynikające z inżynierii społecznej, sposoby rozpoznawania naruszeń bezpieczeństwa oraz znaczenie świadomości użytkowników w ochronie zasobów cyfrowych. Zajęcia rozwijają umiejętność identyfikowania podstawowych zagrożeń, rozumienia zasad poufności, integralności i dostępności danych oraz odpowiedzialnego funkcjonowania w cyberprzestrzeni.	K_W03, K_W06, K_W07, K_W11 K_U04, K_U12 K_K01
Matematyka 1 (semestr 2): W ramach zajęć studenci zapoznają się z wybranymi zagadnieniami matematyki wyższej istotnymi w informatyce i cyberbezpieczeństwie, obejmując m.in. rachunek macierzowy, ciągi i szeregi liczbowe, funkcje rzeczywiste oraz liczby zespolone. Kurs rozwija umiejętności analitycznego myślenia, modelowania i rozwiązywania problemów oraz stosowania narzędzi matematycznych w analizie systemów informatycznych i bezpieczeństwa informacji. Stanowi kontynuację kursu „Wstęp do matematyki", wprowadzając bardziej zaawansowane metody matematyczne wykorzystywane w informatyce i technologiach cyfrowych.	K_W01 K_U01 K_K01
Organizacja i architektura komputerów (semestr 2): W ramach zajęć studenci zapoznają się z podstawowymi rozwiązaniami architektonicznymi cyfrowych układów, zarówno kombinacyjnych, jak i sekwencyjnych, oraz zdobywają umiejętności ich analizy i projektowania w kontekście działania komputerów. Kurs obejmuje również budowę i funkcjonowanie przykładowego komputera, w tym maszyny Von Neumanna, ze sterowaniem sprzętowym i mikroprogramowanym, umożliwiając zrozumienie zasad pracy systemów mikroprocesorowo-komputerowych. Studenci rozwijają wiedzę teoretyczną i praktyczną, przygotowując się do samodzielnej analizy oraz projektowania elementów architektury komputerowej.	K_W02 K_U03, K_U04 K_K01, K_K03
Algorytmy i struktury danych (semestr 2): W ramach zajęć studenci zapoznają się z fundamentalnymi oraz wybranymi zaawansowanymi algorytmami i strukturami danych, które stanowią podstawę współczesnej informatyki i cyberbezpieczeństwa. W ramach kursu omawiane są metody analizy złożoności obliczeniowej, strategie rozwiązywania problemów oraz praktyczna implementacja algorytmów w wybranym języku programowania. Zajęcia rozwijają umiejętności logicznego myślenia, analizy problemów oraz stosowania poznanych metod w różnych zastosowaniach informatycznych i związanych z bezpieczeństwem systemów cyfrowych, przygotowując studentów do tworzenia efektywnych, niezawodnych i bezpiecznych rozwiązań programistycznych.	K_W01, K_W05 K_U01, K_U02 K_K01
Wprowadzenie do sieci komputerowych (semestr 2): W ramach zajęć studenci zapoznają się z podstawowymi pojęciami, technologiami i urządzeniami wykorzystywanymi w budowie oraz administracji sieci komputerowych. Kurs obejmuje podstawy funkcjonowania sieci LAN, WAN i Internetu, model OSI, stos protokołów TCP/IP, zasady adresacji IPv4 i IPv6, konfigurację podstawowych usług sieciowych oraz przegląd urządzeń takich jak routery, przełączniki i punkty dostępowe. Omawiane są również podstawowe techniki diagnostyki sieci, rozwiązywania problemów oraz zagadnienia związane z bezpieczeństwem sieci i ochroną danych. Studenci rozwijają umiejętności projektowania prostych schematów sieci, konfigurowania podstawowych urządzeń sieciowych oraz dobierania narzędzi diagnostycznych do praktycznych problemów.	K_W02, K_W03 K_U03, K_U04 K_K02

Matematyka 2 (semestr 3): W ramach zajęć studenci pogłębiają wiedzę z zakresu analizy matematycznej, ze szczególnym uwzględnieniem funkcji jednej i dwóch zmiennych rzeczywistych. W ramach kursu omawiane są pochodne funkcji, całki oznaczone i nieoznaczone, funkcje wielu zmiennych oraz podstawy równań różniczkowych rzędu pierwszego. Zajęcia rozwijają umiejętność stosowania metod matematycznych w modelowaniu i analizie problemów informatycznych i technicznych. Kurs stanowi naturalną kontynuację „Matematyki 1" i wprowadza narzędzia zaawansowanej analizy matematycznej, przygotowując studentów do zastosowań w programowaniu, uczeniu maszynowym i modelowaniu systemów.	K_W01 K_U01 K_K01
Podstawy kodowania (semestr 3): W ramach zajęć studenci zapoznają się z podstawowymi metodami reprezentacji, kodowania i zabezpieczania informacji w systemach cyfrowych. Kurs obejmuje krótkie przypomnienie wybranych pojęć teorii informacji, takich jak model systemu komunikacyjnego, ilość informacji, entropia oraz źródła wiadomości, a następnie koncentruje się na praktycznych i matematycznych podstawach kodowania danych. Omawiane są metody kodowania źródeł dyskretnych, w tym kody Shannona-Fano i Huffmana, podstawy kompresji bezstratnej, a także wybrane kody służące do wykrywania i korygowania błędów, w tym kody blokowe, macierze generujące i kontrolne, kody Hamminga oraz podstawy kodów cyklicznych. Zajęcia rozwijają umiejętność analizowania efektywności kodów, obliczania podstawowych miar informacji, konstruowania prostych kodów oraz rozumienia znaczenia kodowania w transmisji, przechowywaniu i ochronie danych w systemach informatycznych.	K_W01, K_W04 K_U01, K_U05 K_K01, K_K03
Fizyka i elektronika (semestr 4): W ramach zajęć studenci zapoznają się z fizycznymi podstawami działania wybranych urządzeń i układów wykorzystywanych w informatyce oraz z podstawami teorii obwodów elektrycznych i elektronicznych. Kurs obejmuje zagadnienia dotyczące elektryczności, magnetyzmu, optyki, obwodów prądu stałego i zmiennego, praw Kirchhoffa, rezonansu oraz podstaw działania elementów elektronicznych, takich jak rezystory, kondensatory, cewki, diody, tranzystory i wzmacniacze operacyjne. Omawiane są również półprzewodniki, sensory, przetworniki, elementy optyczne, technologie układów scalonych oraz zastosowania fal elektromagnetycznych w komunikacji bezprzewodowej. Zajęcia rozwijają umiejętności rozwiązywania prostych problemów z zakresu fizyki i elektroniki, projektowania, budowy, uruchamiania i testowania układów elektronicznych oraz posługiwania się podstawowymi narzędziami pomiarowymi.	K_W01, K_W10 K_U01, K_U04 K_K01, K_K02, K_K03
MODUŁ KIERUNKOWY	**EFEKTY KIERUNKOWE**
Teoria bezpieczeństwa (semestr 1): W ramach zajęć studenci zapoznają się z teoretycznymi podstawami nauk o bezpieczeństwie oraz podstawowymi kategoriami terminologicznymi stosowanymi w analizie bezpieczeństwa narodowego i międzynarodowego. Kurs obejmuje współczesne rozumienie bezpieczeństwa, jego przemiany po zakończeniu zimnej wojny, a także przedmiotowe rodzaje bezpieczeństwa, w tym bezpieczeństwo polityczne, militarne, ekonomiczne, społeczne, informacyjne, ekologiczne i zdrowotne. Omawiane są również wyzwania i zagrożenia współczesnego świata, ze szczególnym uwzględnieniem bezpieczeństwa informacyjnego, cyberprzestępczości oraz zagrożeń w cyberprzestrzeni. Zajęcia rozwijają umiejętność krytycznej analizy zjawisk bezpieczeństwa, pracy zespołowej, interpretowania problemów w kontekście politycznym, społecznym, gospodarczym, militarnym, prawnym i etycznym oraz stosowania wybranych metod projektowego rozwiązywania problemów.	K_W06, K_W11 K_U012 K_K04

Programowanie obiektowe (semestr 2): W ramach zajęć studenci zapoznają się z podstawami analizy, projektowania i programowania obiektowego oraz uczą się tworzenia programów w języku C++. Kurs obejmuje podstawowe cechy paradygmatu obiektowego, w tym pojęcie klasy i obiektu, hermetyzację, dziedziczenie, polimorfizm, konstruktory, destruktory, przeciążanie funkcji i operatorów oraz zasady dostępu do pól i metod. Omawiane są również wybrane mechanizmy języka C++, takie jak dynamiczne zarządzanie pamięcią, referencje, wskaźnik `this`, funkcje i zmienne statyczne, obiekty stałe, szablony funkcji i klas, klasy pojemnikowe, iteratory oraz obsługa sytuacji wyjątkowych. Zajęcia rozwijają umiejętność projektowania i implementowania prostych oraz średniozaawansowanych programów obiektowych, kompilowania, uruchamiania i debugowania kodu, a także korzystania z wybranych elementów biblioteki standardowej C++.	K_W05 K_U02 K_K02
Podstawy systemów kontroli wersji i pracy zespołowej w IT (semestr 2): W ramach zajęć studenci zapoznają się z podstawami systemów kontroli wersji oraz zasadami organizacji pracy zespołowej w projektach informatycznych. Kurs obejmuje praktyczne wykorzystanie systemu Git, w tym tworzenie repozytoriów, śledzenie zmian w kodzie, wykonywanie zatwierdzeń, pracę z gałęziami, scalanie zmian, rozwiązywanie konfliktów oraz korzystanie ze zdalnych repozytoriów. Omawiane są również podstawowe zasady współpracy w zespole programistycznym, dokumentowania zmian, zgłaszania i przeglądania zadań, pracy z platformami typu GitHub, GitLab lub Bitbucket oraz stosowania dobrych praktyk w zakresie organizacji kodu i komunikacji projektowej. Zajęcia rozwijają umiejętność samodzielnej i zespołowej pracy nad projektem IT, świadomego zarządzania historią zmian oraz stosowania narzędzi wspierających współpracę, odpowiedzialność za kod i utrzymanie jakości oprogramowania.	K_W09, K_W12 K_U11, K_U14 K_K02, K_K03
Systemy operacyjne (semestr 3): W ramach zajęć studenci zapoznają się z podstawowymi pojęciami, mechanizmami i narzędziami związanymi z działaniem współczesnych systemów operacyjnych, ze szczególnym uwzględnieniem systemów Windows i Linux. Kurs obejmuje zagadnienia dotyczące zarządzania pamięcią, organizacji systemu plików, obsługi urządzeń wejścia/wyjścia, pracy z procesami, synchronizacji procesów, zakleszczeń, strumieni standardowych oraz pracy w systemie operacyjnym z wykorzystaniem konsoli. Omawiane są również elementy diagnostyki i naprawy usterek systemowych i sprzętowych oraz pisanie programów w języku C wykorzystujących funkcje jądra systemu operacyjnego, w tym mechanizmy kolejek komunikatów, pamięci współdzielonej i semaforów. Zajęcia rozwijają umiejętność praktycznej pracy z systemem operacyjnym, analizowania mechanizmów zarządzania zasobami, rozwiązywania problemów systemowych oraz przygotowywania prostych rozwiązań programistycznych współpracujących z systemem.	K_W02, K_W03 K_U03, K_U04 K_K02
Konfiguracja i zarządzanie sieciami komputerowymi (semestr 3): W ramach zajęć studenci pogłębiają wiedzę i umiejętności praktyczne z zakresu projektowania, konfiguracji, wdrażania i zarządzania infrastrukturą sieciową. Kurs obejmuje pracę z profesjonalnymi urządzeniami sieciowymi, konfigurację routerów i przełączników, projektowanie adresacji dla sieci LAN i WAN z wykorzystaniem VLSM i CIDR, organizację routingu statycznego i dynamicznego oraz konfigurację segmentacji sieci z użyciem VLAN. Omawiane są również zagadnienia zdalnego dostępu, usług sieciowych, integracji różnych typów usług w małej organizacji, wykorzystania systemu RouterOS i interfejsu WinBox, konfiguracji urządzeń MikroTik, zabezpieczeń, firewalla, filtrowania ruchu, ochrony przed wybranymi zagrożeniami oraz implementacji VPN. Zajęcia rozwijają umiejętność praktycznej konfiguracji i diagnostyki sieci, testowania rozwiązań w środowiskach laboratoryjnych i symulacyjnych oraz wdrażania podstawowych polityk bezpieczeństwa w infrastrukturze sieciowej.	K_W02, K_W03 K_U03, K_U04, K_U07 K_K02

Wprowadzenie do technologii chmury (semestr 3): W ramach zajęć studenci zapoznają się z podstawowymi koncepcjami, architekturą i sposobami wykorzystania chmury obliczeniowej we współczesnych systemach informatycznych. Kurs obejmuje modele usług chmurowych, w tym IaaS, PaaS i SaaS, modele wdrożeń chmury publicznej, prywatnej i hybrydowej, a także przegląd podstawowych usług oferowanych przez wybrane platformy chmurowe, takich jak zasoby obliczeniowe, przechowywanie danych, usługi sieciowe, bazy danych oraz mechanizmy zarządzania środowiskiem. Omawiane są również podstawy uruchamiania i konfigurowania zasobów w chmurze, zasady skalowania usług, rozliczania kosztów, organizacji kont i projektów oraz typowe scenariusze wykorzystania chmury w aplikacjach internetowych, systemach biznesowych i środowiskach testowych. Zajęcia rozwijają umiejętność rozumienia architektury rozwiązań chmurowych, dobierania podstawowych usług do prostych potrzeb projektowych oraz świadomego korzystania z infrastruktury chmurowej jako elementu współczesnego środowiska IT.	K_W02, K_W10 K_U03, K_U04 K_K01
Standaryzacja systemów cyberbezpieczeństwa (semestr 3): W ramach zajęć studenci zapoznają się z podstawami standaryzacji systemów cyberbezpieczeństwa oraz z normami i dobrymi praktykami stosowanymi przy wdrażaniu, utrzymaniu i doskonaleniu systemów bezpieczeństwa informacji. Kurs obejmuje wprowadzenie do metodologii standaryzacji, rolę instytucji i organizacji normalizacyjnych, znaczenie certyfikatów, zakresy stosowania standardów oraz podstawy normy PN-EN ISO/IEC 27001 dotyczącej Systemu Zarządzania Bezpieczeństwem Informacji. Omawiane są również procesy wdrażania systemów bezpieczeństwa w organizacjach, szacowanie ryzyka, analiza zagrożeń, dobór mechanizmów ochrony, monitorowanie zgodności oraz metody ciągłego doskonalenia. Zajęcia rozwijają umiejętność interpretowania norm bezpieczeństwa, przygotowywania polityk i procedur bezpieczeństwa, formułowania rekomendacji oraz pracy zespołowej przy projektach związanych ze standaryzacją i audytem cyberbezpieczeństwa.	K_W06, K_W12 K_U06, K_U12, K_U13 K_K02
Podstawy sztucznej inteligencji (semestr 4): W ramach zajęć studenci zapoznają się z wybranymi metodami sztucznej inteligencji oraz ich zastosowaniami w rozwiązywaniu problemów informatycznych i analitycznych. Kurs obejmuje podstawowe pojęcia i koncepcje sztucznej inteligencji, w tym test Turinga, rozróżnienie między silną i słabą sztuczną inteligencją, reprezentację wiedzy, wnioskowanie, systemy ekspertowe, metody wyszukiwania i rozwiązywania problemów oraz wybrane zagadnienia przetwarzania języka naturalnego. Omawiane są również metody rozpoznawania wzorców, podstawy uczenia maszynowego, w tym drzewa decyzyjne, metody zespołowe, regresja, klasyfikatory oparte na odległości, a także podstawy sztucznych sieci neuronowych, od neuronów logicznych i uczenia Hebba po sieci jednokierunkowe. Zajęcia rozwijają umiejętność implementowania wybranych algorytmów sztucznej inteligencji, przygotowywania danych do analizy, doboru metod AI do problemu oraz krytycznej oceny wyników, także w kontekście zastosowań związanych z analizą informacji, klasyfikacją treści i cyberbezpieczeństwem.	K_W01, K_W08 K_U09, K_U10 K_K01
Bazy danych (semestr 4): W ramach zajęć studenci zapoznają się z podstawami organizacji, modelowania, przetwarzania i przechowywania danych z wykorzystaniem systemów bazodanowych. Kurs obejmuje podstawowe pojęcia dotyczące relacyjnych baz danych, w tym tabele, pola, rekordy, typy danych, klucze, klucze obce, związki encji, diagramy ERD oraz reguły integralności. Omawiane są modele danych, systemy zarządzania bazami danych, podstawowe i zaawansowane konstrukcje języka SQL, normalizacja, denormalizacja, indeksowanie, transakcje, zarządzanie równoczesnością oraz podstawy administracji bazami danych, w tym tworzenie użytkowników, zarządzanie dostępem i wykonywanie kopii zapasowych. Zajęcia rozwijają umiejętność projektowania struktur baz danych, formułowania zapytań SQL, optymalizacji modelu danych oraz tworzenia prostych aplikacji wykorzystujących bazę danych.	K_W02, K_W03 K_U03, K_U04 K_K01, K_K03

Bezpieczeństwo systemów operacyjnych (semestr 4): W ramach zajęć studenci zapoznają się z praktycznymi metodami zabezpieczania systemów operacyjnych oraz ochrony danych i prywatności użytkowników. Kurs obejmuje analizę zagrożeń systemowych, modele polityk bezpieczeństwa, wykorzystanie narzędzi systemowych i niezależnych programów do zabezpieczania systemu, konfigurowanie i testowanie zapór sieciowych, bezpieczne korzystanie z usług oraz stosowanie silnego szyfrowania i uwierzytelniania. Omawiane są również zagadnienia monitorowania działania sieci i systemu, wykrywania obecności intruzów, identyfikowania naruszeń bezpieczeństwa oraz przywracania poprawnego funkcjonowania systemu po incydencie. Zajęcia rozwijają umiejętność praktycznego stosowania mechanizmów ochrony systemów operacyjnych, wykrywania i ograniczania skutków incydentów oraz odpowiedzialnego zarządzania bezpieczeństwem środowiska systemowego.	K_W02, K_W03, K_W07 K_U03, K_U04, K_U07 K_K02
Bezpieczeństwo sieci komputerowych (semestr 4): W ramach zajęć studenci zapoznają się z zasadami zabezpieczania lokalnych i rozległych sieci komputerowych oraz z praktycznymi metodami ograniczania ryzyka w infrastrukturze sieciowej. Kurs obejmuje podstawową konfigurację urządzeń sieciowych, przełączanie ramek, wirtualne sieci LAN, routing między VLAN-ami, protokoły drzewa opinającego, agregację portów, DHCP dla IPv4 i IPv6, routing statyczny, jednoobszarowy OSPFv2, listy kontroli dostępu, translację adresów sieciowych oraz wirtualne sieci prywatne z wykorzystaniem IPSec. Omawiane są również zagadnienia bezpieczeństwa sieci LAN i sieci bezprzewodowych, monitorowania i zarządzania siecią, automatyzacji sieci, ochrony z użyciem rozwiązań IPS, szyfrowania, bezpieczeństwa stacji końcowych, poczty elektronicznej, ochrony tożsamości, łamania haseł, wykrywania anomalii oraz zabezpieczeń w warstwie DNS. Zajęcia rozwijają umiejętność konfigurowania urządzeń i protokołów sieciowych, projektowania bezpiecznych topologii oraz analizowania i wdrażania zabezpieczeń w praktycznych środowiskach teleinformatycznych.	K_W02, K_W03, K_W04, K_W07 K_U03, K_U04, K_U06, K_U07 K_K02
Militarny wymiar cyberbezpieczeństwa (semestr 4): W ramach zajęć studenci zapoznają się z militarnym znaczeniem cyberprzestrzeni jako współczesnej domeny prowadzenia działań, rywalizacji i konfliktów między państwami oraz innymi podmiotami bezpieczeństwa. Kurs obejmuje podstawowe pojęcia związane z cyberobroną, cyberatakami, wojną hybrydową, operacjami informacyjnymi, ochroną infrastruktury krytycznej oraz rolą sił zbrojnych i instytucji państwowych w zapewnianiu bezpieczeństwa cyberprzestrzeni. Omawiane są również przykłady wykorzystania działań cybernetycznych w konfliktach zbrojnych i kryzysach międzynarodowych, znaczenie odporności państwa na zakłócenia cyfrowe, współpraca cywilno-wojskowa oraz podstawowe uwarunkowania prawne, organizacyjne i strategiczne cyberbezpieczeństwa w wymiarze narodowym, sojuszniczym i międzynarodowym. Zajęcia rozwijają umiejętność analizy zagrożeń cybernetycznych w kontekście bezpieczeństwa państwa, oceny skutków działań w cyberprzestrzeni oraz interpretowania cyberbezpieczeństwa jako elementu współczesnej strategii obronnej.	K_W06, K_W11, K_U12, K_U13 K_K04
Bezpieczeństwo baz danych (semestr 5): W ramach zajęć studenci zapoznają się z praktycznymi metodami zabezpieczania systemów bazodanowych oraz danych przechowywanych i przetwarzanych w bazach danych. Kurs obejmuje zarządzanie kontami użytkowników, rolami i uprawnieniami, kontrolę dostępu do obiektów bazy danych, zasady minimalnych uprawnień, zabezpieczanie połączeń z bazą, konfigurację podstawowych mechanizmów audytu oraz monitorowanie aktywności użytkowników. Omawiane są również zagadnienia kopii zapasowych i odtwarzania danych, szyfrowania danych i połączeń, integralności danych, ochrony przed nieautoryzowanym dostępem oraz wybranych podatności aplikacji korzystających z baz danych, w tym wstrzykiwania kodu SQL. Zajęcia rozwijają umiejętność praktycznej konfiguracji zabezpieczeń w wybranym systemie zarządzania bazą danych, diagnozowania błędów konfiguracyjnych, analizowania ryzyka związanego z dostępem do danych oraz stosowania dobrych praktyk w zakresie ochrony poufności, integralności i dostępności danych.	K_W02, K_W03, K_W04 K_U03, K_U04, K_U05 K_K02

Kryptografia (semestr 5): W ramach zajęć studenci zapoznają się z historią, podstawowymi pojęciami oraz metodami kryptografii i kryptoanalizy. Kurs obejmuje podstawowe elementy kryptologii, proste szyfry, szyfrowanie z kluczem, szyfrowanie symetryczne i asymetryczne, a także wybrane algorytmy symetryczne, w tym DES, Triple DES, Blowfish, CAST, IDEA, RC2, RC4, RC5, RC6, Rijndael oraz AES. Omawiane są również tryby pracy szyfrów blokowych, takie jak ECB, CBC, CFB, OFB i tryb licznikowy, algorytm RSA, funkcje skrótu, w tym MD4, MD5, SHA-1, SHA-2 i SHA-3, podpis cyfrowy oraz podstawowe techniki łamania szyfrów. Zajęcia rozwijają umiejętność rozumienia, projektowania, implementowania i analizowania podstawowych mechanizmów kryptograficznych stosowanych w ochronie danych oraz systemach bezpieczeństwa informatycznego.	K_W01, K_W04 K_U01, K_U05 K_K01
Bezpieczeństwo aplikacji internetowych (semestr 5): W ramach zajęć studenci zapoznają się z najważniejszymi zagrożeniami bezpieczeństwa aplikacji internetowych oraz z praktycznymi metodami ich wykrywania, testowania i ograniczania. Kurs obejmuje typowe podatności aplikacji webowych, w tym zagadnienia z grupy OWASP Top 10, ataki SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, przechwytywanie sesji, nieuprawniony dostęp do obiektów, ujawnienie danych wrażliwych oraz wybrane techniki ataków DoS i DDoS. Omawiane są również metody zabezpieczania aplikacji, w tym walidacja danych wejściowych, stosowanie zapytań parametryzowanych i ORM, zasady secure coding, bezpieczne przechowywanie i weryfikacja haseł, mechanizmy uwierzytelniania i kontroli dostępu, bezpieczeństwo sesji, JWT, OAuth2, konfiguracja SSL/TLS, certyfikaty x.509, mechanizmy zabezpieczeń przeglądarki, Web Application Firewall oraz narzędzia wspomagające diagnostykę podatności. Zajęcia rozwijają umiejętność identyfikowania luk bezpieczeństwa, testowania aplikacji internetowych, wdrażania mechanizmów obrony oraz projektowania aplikacji webowych z uwzględnieniem bezpieczeństwa już na etapie implementacji.	K_W03, K_W04, K_W05 K_U03, K_U04, K_U05, K_U06 K_K02
Inżynieria odwrotna (semestr 5): W ramach zajęć studenci zapoznają się z podstawami inżynierii odwrotnej oprogramowania oraz z jej zastosowaniem w analizie i zabezpieczaniu rozwiązań informatycznych. Kurs obejmuje techniki analizy gotowego oprogramowania, dekompilacji, rekonstrukcji kodu źródłowego, analizy kodu maszynowego i kodu pośredniego, a także badania programów skryptowych, formatów zapisu danych oraz protokołów komunikacyjnych. Omawiane są narzędzia wykorzystywane w inżynierii odwrotnej, w tym disassemblery, debuggery, edytory heksadecymalne, sniffery i narzędzia systemowe, jak również techniki zabezpieczania aplikacji, takie jak obfuskacja kodu wynikowego. Zajęcia rozwijają umiejętność praktycznego posługiwania się narzędziami inżynierii odwrotnej, rozumienia wpływu procesu wytwarzania oprogramowania na możliwość jego analizy oraz oceny prawnych i etycznych aspektów stosowania tych technik.	K_W05, K_W07 K_U06, K_U08 K_K02
Zarządzanie projektami cyberbezpieczeństwa (semestr 5): W ramach zajęć studenci zapoznają się z podstawami zarządzania projektami realizowanymi w obszarze cyberbezpieczeństwa oraz z organizacją pracy zespołów odpowiedzialnych za wdrażanie rozwiązań bezpieczeństwa. Kurs obejmuje definiowanie celów i zakresu projektu, identyfikację interesariuszy, planowanie zadań, harmonogramowanie prac, szacowanie zasobów, podział odpowiedzialności, monitorowanie postępów oraz przygotowywanie podstawowej dokumentacji projektowej. Omawiane są również zagadnienia zarządzania ryzykiem, komunikacji w projekcie, kontroli zmian, wymagań bezpieczeństwa, zgodności z procedurami organizacyjnymi oraz oceny skuteczności wdrażanych rozwiązań. Zajęcia rozwijają umiejętność planowania i prowadzenia projektów z zakresu cyberbezpieczeństwa, przygotowywania dokumentacji, pracy zespołowej oraz łączenia perspektywy technicznej, organizacyjnej i zarządczej w realizacji przedsięwzięć IT.	K_W06, K_W12 K_U12, K_U13, K_U14 K_K03, K_K04

Metody zbierania informacji (semestr 5): W ramach zajęć studenci zapoznają się z metodami pozyskiwania informacji i danych z różnych źródeł, zarówno automatycznych, jak i opartych na interakcji z użytkownikami. Kurs obejmuje źródła i klasyfikację danych, w tym dane pierwotne i wtórne, ustrukturyzowane i nieustrukturyzowane, dane publiczne, otwarte i komercyjne, a także podstawowe techniki ich pozyskiwania. Omawiane są praktyczne metody web scrapingu, pobierania danych z interfejsów API, pracy z formatami JSON i CSV, projektowania formularzy i ankiet, oceny kompletności, spójności i wiarygodności danych oraz organizacji, przechowywania, automatyzacji pobierania i wykonywania kopii zapasowych. Zajęcia rozwijają umiejętność wykorzystywania narzędzi języka Python do pozyskiwania i porządkowania danych, dobierania metody zbierania informacji do problemu oraz odpowiedzialnego korzystania ze źródeł z uwzględnieniem aspektów prawnych, etycznych i jakościowych.	K_W03, K_W07 K_U07, K_U08, K_U13 K_K02
Wojny informacyjne (semestr 5): W ramach zajęć studenci zapoznają się z podstawowymi pojęciami, strategiami i narzędziami stosowanymi we współczesnych wojnach informacyjnych. Kurs obejmuje klasyfikację i metody wojen informacyjnych, dezinformację jako element wojny hybrydowej, specyfikę broni informacyjnej, ataki socjotechniczne, rolę białego wywiadu oraz sposoby identyfikowania operacji informacyjnych w środowisku cyfrowym i społecznym. Omawiane są również modele grafowe, modele sieciowe i duże modele językowe jako narzędzia analizy oraz modelowania procesów informacyjno-psychologicznych w kontekście konfliktów, rywalizacji państw i działań destabilizacyjnych. Zajęcia rozwijają umiejętność rozpoznawania schematów działań przeciwnika w cyberprzestrzeni, analizowania kampanii informacyjnych, identyfikowania pułapek poznawczych oraz oceny i przeciwdziałania operacjom informacyjnym.	K_W06, K_W11, K_W05 K_U12, K_U13 K_K04
Podstawy prawne cyberbezpieczeństwa (semestr 5): W ramach zajęć studenci zapoznają się z podstawowymi regulacjami prawnymi dotyczącymi cyberbezpieczeństwa, ochrony informacji oraz odpowiedzialności podmiotów funkcjonujących w cyberprzestrzeni. Kurs obejmuje krajowe i europejskie podstawy prawne cyberbezpieczeństwa, w tym zagadnienia związane z krajowym systemem cyberbezpieczeństwa, ochroną danych osobowych, obowiązkami administratorów systemów informacyjnych, bezpieczeństwem usług cyfrowych, ochroną infrastruktury krytycznej oraz reagowaniem na incydenty. Omawiane są również podstawowe pojęcia prawne dotyczące przestępczości komputerowej, odpowiedzialności karnej, cywilnej i administracyjnej, obowiązków raportowania naruszeń oraz zasad współpracy między instytucjami publicznymi, przedsiębiorcami i podmiotami odpowiedzialnymi za bezpieczeństwo informacji. Zajęcia rozwijają umiejętność interpretowania podstawowych wymagań prawnych w obszarze cyberbezpieczeństwa, rozpoznawania obowiązków organizacji oraz analizowania problemów bezpieczeństwa cyfrowego w kontekście norm prawnych, organizacyjnych i etycznych.	K_W06 K_U12, K_U13 K_K02, K_K04
Technologie decentralizacji danych (Blockchain) (semestr 7): W ramach zajęć studenci zapoznają się z podstawami technologii blockchain oraz mechanizmami decentralizacji danych wykorzystywanymi we współczesnych systemach rozproszonych. Kurs obejmuje architekturę sieci blockchain, strukturę łańcucha bloków, sposoby zapisu i weryfikacji danych, mechanizmy konsensusu, rolę kryptografii w zapewnianiu integralności i niezmienności danych oraz zasady działania zdecentralizowanych rejestrów. Omawiane są również smart kontrakty, ich zastosowania, wybrane problemy bezpieczeństwa, możliwości i ograniczenia systemów blockchain oraz przykłady wykorzystania technologii decentralizacji danych w różnych obszarach IT. Zajęcia rozwijają umiejętność rozumienia architektury systemów blockchain, analizowania zastosowań zdecentralizowanego przechowywania i przetwarzania danych oraz oceny ryzyka związanego z bezpieczeństwem, skalowalnością i wiarygodnością rozwiązań opartych na rejestrach rozproszonych.	K_W14 K_U16 K_K01

Technologie wykrywania i zapobiegania cyberatakom (semestr 7): W ramach zajęć studenci zapoznają się z technologiami wykorzystywanymi do monitorowania bezpieczeństwa, wykrywania cyberataków oraz ograniczania ich skutków w środowiskach teleinformatycznych. Kurs obejmuje źródła danych bezpieczeństwa, w tym logi systemowe, sieciowe i aplikacyjne, zdarzenia z urządzeń bezpieczeństwa oraz podstawy analizy ruchu sieciowego w kontekście identyfikacji podejrzanych aktywności. Omawiane są systemy IDS i IPS, rozwiązania klasy SIEM, mechanizmy korelacji zdarzeń, reguły detekcji, wskaźniki kompromitacji, podstawy threat intelligence oraz metody klasyfikacji i priorytetyzacji alertów. Zajęcia rozwijają umiejętność praktycznej analizy zdarzeń bezpieczeństwa, interpretowania alertów, przygotowywania prostych reguł detekcji oraz dobierania technologii wspierających wykrywanie i ograniczanie cyberataków w pracy zespołów monitorowania bezpieczeństwa.	K_W06, K_W14 K_U12, K_U16 K_K02
Metodyki testów penetracyjnych (semestr 7): W ramach zajęć studenci zapoznają się z metodycznym podejściem do planowania, prowadzenia i dokumentowania testów penetracyjnych systemów informatycznych. Kurs obejmuje podstawowe pojęcia związane z testami bezpieczeństwa, klasyfikację testów penetracyjnych, określanie zakresu i celu badania, zasady pracy w środowisku autoryzowanym, etapy rozpoznania, identyfikacji podatności, weryfikacji podatności, oceny ryzyka oraz przygotowywania rekomendacji naprawczych. Omawiane są również wybrane metodyki i standardy prowadzenia testów, zasady bezpiecznego korzystania z narzędzi wspierających testy penetracyjne, analiza podatności systemów, sieci i aplikacji, dokumentowanie wyników oraz przygotowanie raportu technicznego i zarządczego. Zajęcia rozwijają umiejętność planowania testu penetracyjnego, dobierania technik i narzędzi do badanego środowiska, interpretowania wyników, formułowania wniosków oraz prowadzenia działań testowych zgodnie z zasadami prawa, etyki i odpowiedzialności zawodowej.	K_W06, K_W11 K_U13, K_U15 K_K01, K_K03, K_K04
MODUŁ KURSÓW OBIERALNYCH	**EFEKTY KIERUNKOWE**
Języki skryptowe (semestr 1): W ramach zajęć studenci zapoznają się z podstawami języków skryptowych oraz ich zastosowaniem w informatyce i cyberbezpieczeństwie. Kurs obejmuje wprowadzenie do języków Python i Bash, tworzenie prostych skryptów, pracę z plikami i katalogami, wykorzystanie bibliotek oraz integrację różnych środowisk skryptowych. Szczególną uwagę poświęca się automatyzacji zadań administracyjnych, analizie danych, monitorowaniu systemów oraz wspomaganiu wybranych działań związanych z bezpieczeństwem systemów komputerowych. Studenci rozwijają praktyczne umiejętności pisania skryptów użytkowych, dobierania narzędzi do realizacji zadań oraz samodzielnego usprawniania pracy w środowisku systemowym.	K_W05 K_U02 K_K02
Programowanie funkcyjne (Python) (semestr 1): W ramach zajęć studenci zapoznają się z podstawami programowania w języku Python, ze szczególnym uwzględnieniem paradygmatu programowania funkcyjnego. Kurs obejmuje podstawowe elementy składni języka Python, typy danych, kolekcje, instrukcje sterujące, definiowanie funkcji oraz wybrane moduły i pakiety. Następnie omawiane są najważniejsze idee programowania funkcyjnego, w tym funkcje jako obiekty pierwszej klasy, funkcje anonimowe, funkcje wyższego rzędu, rekurencja, listy składane, wyrażenia generatorowe oraz wykorzystanie modułu functools. Zajęcia rozwijają umiejętność tworzenia czytelnych i poprawnych programów, łączenia podejścia proceduralnego i funkcyjnego oraz stosowania abstrakcyjnego myślenia w rozwiązywaniu problemów obliczeniowych.	K_W05 K_U02 K_K02

Programowanie systemowe (C lub C++) (semestr 2): W ramach zajęć studenci zapoznają się z podstawami programowania systemowego, ze szczególnym uwzględnieniem środowiska Unix/Linux oraz języków C/C++. Kurs obejmuje korzystanie z terminala systemu operacyjnego, pracę z katalogami, plikami, linkami, uprawnieniami, procesami, sygnałami, potokami i strumieniami, a także podstawy automatyzacji zadań systemowych za pomocą skryptów powłoki Bash. Omawiane są różnice między programowaniem użytkowym a systemowym, wykorzystanie bibliotek i funkcji systemowych Unix/Linux, kompilacja i testowanie programów, operacje wejścia/wyjścia, obsługa deskryptorów plików i błędów oraz tworzenie i synchronizacja procesów. Zajęcia rozwijają umiejętność tworzenia, uruchamiania, testowania i analizowania programów systemowych, a także pisania bezpiecznego i wydajnego kodu współpracującego bezpośrednio z zasobami systemu operacyjnego.	K_W02, K_W05 K_U02, K_U03 K_K02
Języki hipertekstowe i tworzenie stron WWW (semestr 2): W ramach zajęć studenci zapoznają się z podstawami tworzenia stron internetowych z wykorzystaniem języków opisu stron oraz arkuszy stylów. Kurs obejmuje strukturę dokumentu HTML/XHTML, podstawowe znaczniki tekstowe, elementy semantyczne, formatowanie treści za pomocą CSS, zasady kaskady, selektory, układ elementów na stronie, tworzenie menu, formularzy oraz wykorzystanie grafiki i multimediów. Omawiane są również standardy publikowane przez W3C, narzędzia do walidacji kodu, podstawy użyteczności, dostępności i responsywności stron, w tym zastosowanie technik takich jak flexbox, grid oraz zapytania medialne. Zajęcia rozwijają praktyczne umiejętności projektowania, tworzenia, weryfikowania i uruchamiania stron WWW, a także zwracają uwagę na podstawowe aspekty zabezpieczania i optymalizacji serwisów internetowych.	K_W03, K_W05 K_U02, K_U03 K_K02
Technologie DevSecOps (semestr 3): W ramach zajęć studenci zapoznają się z koncepcją DevSecOps, czyli podejściem integrującym wytwarzanie oprogramowania, administrację środowiskami uruchomieniowymi oraz bezpieczeństwo aplikacji w całym cyklu życia systemu. Kurs obejmuje organizację pracy zespołowej z wykorzystaniem systemów kontroli wersji, automatyzację procesów budowania, testowania i wdrażania aplikacji, projektowanie potoków CI/CD oraz włączanie mechanizmów bezpieczeństwa do kolejnych etapów procesu dostarczania oprogramowania. Omawiane są również zagadnienia statycznej i dynamicznej analizy bezpieczeństwa aplikacji, kontroli podatności w zależnościach, zarządzania sekretami, bezpieczeństwa obrazów kontenerowych, podstaw infrastruktury jako kodu, monitorowania, logowania oraz audytowalności procesu wdrożeniowego. Zajęcia rozwijają umiejętność projektowania bezpiecznych i powtarzalnych procesów dostarczania aplikacji, automatyzowania kontroli jakości i bezpieczeństwa oraz identyfikowania ryzyka wynikającego z błędów konfiguracyjnych, podatności kodu i niewłaściwego zarządzania środowiskami.	K_W09, K_W12 K_U11, K_U13, K_U14 K_K02, K_K03
Programowanie niskopoziomowe (semestr 3): W ramach zajęć studenci zapoznają się z podstawami programowania niskopoziomowego oraz z mechanizmami działania kodu na poziomie bliższym architekturze sprzętowej komputera. Kurs obejmuje różnice między programowaniem wysokopoziomowym i niskopoziomowym, podstawy architektury procesora, pracę z pamięcią, rejestrami i instrukcjami, a także analizę kodu generowanego przez kompilator. Omawiane są narzędzia wspierające pracę programisty, w tym kompilatory, debuggery, narzędzia do śledzenia wykonania programu, deasemblery i analizatory binarne, a także zagadnienia związane z optymalizacją kodu, obsługą sprzętu, przerwaniami oraz mechanizmami zarządzania pamięcią. Szczególną uwagę poświęca się analizie bezpieczeństwa i podatności w kodzie, w tym przepełnieniom bufora, analizie błędów pamięci oraz bezpiecznym praktykom programistycznym w kontekście niskopoziomowym.	K_W02, K_W05 K_U02, K_U03 K_K02

Programowanie aplikacji internetowych (Java) (semestr 3): W ramach zajęć studenci zapoznają się z podstawami programowania w języku Java oraz z zasadami tworzenia aplikacji internetowych. Kurs obejmuje składnię języka Java, kompilację i uruchamianie programów, podstawowe mechanizmy programowania obiektowego, w tym klasy, hermetyzację, dziedziczenie, polimorfizm, konstruktory, modyfikatory dostępu, pola i metody statyczne, obsługę wyjątków, typy generyczne oraz kolekcje. Następnie omawiane są technologie wykorzystywane przy tworzeniu aplikacji internetowych, w tym serwer aplikacji, kontener Java Enterprise Edition, serwlety, obsługa żądań i odpowiedzi, sesje, ciasteczka, połączenie z bazą danych przez JDBC, JSP, JSF, JPA oraz podstawy Spring i Spring Boot. Zajęcia rozwijają umiejętność projektowania, implementowania, testowania i wdrażania aplikacji internetowych w języku Java, z uwzględnieniem zasad bezpieczeństwa, pracy zespołowej i dokumentowania rozwiązań programistycznych.	K_W03, K_W05 K_U02, K_U03 K_K02
Teoria zarządzania ryzykiem cyberbezpieczeństwa (semestr 4): W ramach zajęć studenci zapoznają się z podstawami zarządzania ryzykiem cyberbezpieczeństwa w systemach informacyjnych i teleinformatycznych. Kurs obejmuje pojęcia zasobu, zagrożenia, podatności, incydentu, wpływu, prawdopodobieństwa, poziomu ryzyka, ryzyka rezydualnego oraz akceptowalnego poziomu ryzyka. Omawiane są etapy procesu zarządzania ryzykiem, w tym identyfikacja i klasyfikacja zasobów, rozpoznawanie zagrożeń i podatności, szacowanie prawdopodobieństwa i skutków, ocena poziomu ryzyka oraz wybór sposobu postępowania z ryzykiem. Zajęcia rozwijają umiejętność stosowania metod jakościowej i podstawowej ilościowej oceny ryzyka, przygotowywania rejestru ryzyka, proponowania adekwatnych środków zaradczych oraz uzasadniania decyzji dotyczących ograniczania, przenoszenia, akceptowania lub unikania ryzyka.	K_W06, K_W12 K_U06, K_U12, K_U14 K_K04
Przetwarzanie sygnałów (semestr 4): W ramach zajęć studenci zapoznają się z podstawami reprezentacji, analizy i przetwarzania sygnałów dyskretnych oraz ich zastosowaniami w informatyce, systemach technicznych i cyberbezpieczeństwie. Kurs obejmuje podstawowe pojęcia związane z sygnałem, próbkowaniem, kwantyzacją, szumem, analizą w dziedzinie czasu i częstotliwości, filtracją oraz wykrywaniem zmian i anomalii w danych sygnałowych. Omawiane są również wybrane metody numerycznego przetwarzania sygnałów, w tym transformata Fouriera, podstawy analizy widmowej, filtracja cyfrowa, wygładzanie danych, ekstrakcja cech oraz interpretacja wyników w kontekście danych pomiarowych, telemetrycznych, sieciowych lub systemowych. Zajęcia rozwijają umiejętność praktycznej analizy sygnałów z wykorzystaniem narzędzi programistycznych, przygotowywania danych do dalszego przetwarzania, identyfikowania zakłóceń i nietypowych wzorców oraz stosowania podstawowych metod przetwarzania sygnałów w zadaniach diagnostycznych i analitycznych.	K_W01, K_W10 K_U01, K_U04 K_K01, K_K03
Bezpieczeństwo technologii chmurowych (semestr 4): W ramach zajęć studenci zapoznają się z metodami zabezpieczania środowisk chmurowych oraz z najważniejszymi zagrożeniami wynikającymi z wykorzystywania usług cloud computing. Kurs obejmuje modele odpowiedzialności za bezpieczeństwo w chmurze, zarządzanie tożsamością i dostępem, zasadę minimalnych uprawnień, bezpieczną konfigurację zasobów obliczeniowych, magazynów danych, usług sieciowych i kont administracyjnych, a także ochronę danych przetwarzanych w środowiskach publicznych, prywatnych i hybrydowych. Omawiane są również zagadnienia szyfrowania danych, zarządzania kluczami, monitorowania aktywności, logowania zdarzeń, wykrywania błędnych konfiguracji, reagowania na incydenty, wykonywania kopii zapasowych, zapewniania ciągłości działania oraz zgodności z wymaganiami prawnymi i organizacyjnymi. Zajęcia rozwijają umiejętność praktycznej analizy bezpieczeństwa środowiska chmurowego, konfigurowania podstawowych mechanizmów ochrony, identyfikowania ryzyka związanego z usługami chmurowymi oraz dobierania zabezpieczeń do typowych scenariuszy wykorzystania chmury w organizacji.	K_W02, K_W03, K_W10 K_U03, K_U04, K_U06 K_K02

Metody i narzędzia zabezpieczania aplikacji AI (semestr 5): W ramach zajęć studenci zapoznają się z metodami i narzędziami zabezpieczania aplikacji wykorzystujących sztuczną inteligencję oraz uczenie maszynowe. Kurs koncentruje się na bezpieczeństwie warstwy aplikacyjnej, interfejsów programistycznych, danych wejściowych i wyjściowych oraz integracji modeli AI z systemami informatycznymi. Omawiane są zagadnienia walidacji danych, kontroli dostępu, ochrony endpointów modelu, zabezpieczania API, zarządzania sekretami, logowania zdarzeń, ograniczania nadużyć, monitorowania działania aplikacji oraz ochrony danych wykorzystywanych przez aplikacje AI. Zajęcia rozwijają umiejętność praktycznego identyfikowania ryzyk w aplikacjach korzystających z AI, wdrażania podstawowych mechanizmów zabezpieczających, testowania poprawności konfiguracji oraz przygotowywania rekomendacji ograniczających ryzyko techniczne, organizacyjne i prawne.	K_W03, K_W08, K_W10 K_U06, K_U10 K_K02
Bezpieczeństwo systemów AI i LLM (semestr 5): W ramach zajęć studenci zapoznają się z zagrożeniami, podatnościami i mechanizmami ochrony charakterystycznymi dla systemów sztucznej inteligencji oraz dużych modeli językowych. Kurs obejmuje specyfikę bezpieczeństwa modeli uczenia maszynowego i systemów generatywnej AI, w tym ryzyka związane z danymi treningowymi, zatruwaniem danych, przykładami adwersarialnymi, ekstrakcją modelu, inferencją o danych, ujawnianiem informacji oraz niekontrolowanym wykorzystaniem wyników działania modelu. Omawiane są również zagrożenia właściwe aplikacjom opartym na LLM, takie jak prompt injection, jailbreak, halucynacje, wycieki danych, manipulacja kontekstem, podatności systemów RAG, ryzyka związane z użyciem narzędzi przez agentów AI oraz problemy kontroli dostępu do źródeł danych i funkcji systemu. Zajęcia rozwijają umiejętność testowania odporności systemów AI i LLM, projektowania podstawowych zabezpieczeń, oceny ryzyka, monitorowania zachowania modeli, przygotowywania scenariuszy nadużyć oraz formułowania rekomendacji ograniczających ryzyko techniczne, organizacyjne, prawne i etyczne.	K_W03, K_W08 K_U09, K_U10 K_K02
Bezpieczeństwo systemów elektronicznych (semestr 5): W ramach zajęć studenci zapoznają się z podstawami bezpieczeństwa systemów elektronicznych, urządzeń wbudowanych oraz elementów infrastruktury sprzętowej wykorzystywanej w systemach informatycznych i teleinformatycznych. Kurs obejmuje zagrożenia wynikające z fizycznego dostępu do urządzeń, błędów konfiguracji, nieodpowiedniego zabezpieczenia interfejsów diagnostycznych, podatności firmware'u, niezabezpieczonej komunikacji oraz niewłaściwego zarządzania aktualizacjami i cyklem życia urządzeń. Omawiane są również podstawowe metody identyfikacji komponentów elektronicznych, analiza dokumentacji technicznej, zabezpieczanie portów i interfejsów komunikacyjnych, ochrona urządzeń IoT i systemów wbudowanych, bezpieczne uruchamianie, kontrola dostępu, szyfrowanie komunikacji oraz wykrywanie typowych błędów projektowych i eksploatacyjnych. Zajęcia rozwijają umiejętność praktycznej analizy bezpieczeństwa prostych systemów elektronicznych, identyfikowania potencjalnych wektorów ataku, oceny ryzyka związanego z eksploatacją urządzeń oraz dobierania podstawowych mechanizmów ochrony sprzętu, oprogramowania układowego i komunikacji urządzeń.	K_W02, K_W03, K_W10 K_U04, K_U06 K_K02
AI w reagowaniu na incydenty w kryminalistyce cyfrowej (semestr 5): W ramach zajęć studenci zapoznają się z możliwościami wykorzystania metod sztucznej inteligencji w reagowaniu na incydenty bezpieczeństwa oraz w wybranych zadaniach kryminalistyki cyfrowej. Kurs obejmuje podstawowe etapy obsługi incydentu, zabezpieczanie i analizę materiału cyfrowego, pracę z logami, danymi systemowymi, sieciowymi i aplikacyjnymi oraz wykorzystanie narzędzi AI do klasyfikacji zdarzeń, wykrywania anomalii, korelacji informacji, priorytetyzacji alertów i wspomagania analizy śladów cyfrowych. Omawiane są również zastosowania uczenia maszynowego i dużych modeli językowych w analizie raportów, dokumentacji, komunikacji, próbek danych oraz scenariuszy incydentów, z uwzględnieniem ograniczeń, ryzyka błędnej interpretacji wyników, ochrony danych oraz wymagań dotyczących integralności i wiarygodności materiału dowodowego. Zajęcia rozwijają umiejętność praktycznego wykorzystywania narzędzi AI jako wsparcia pracy analityka, formułowania hipotez dotyczących przebiegu incydentu, dokumentowania działań oraz krytycznej oceny wyników generowanych przez systemy automatyczne.	K_W07, K_W08 K_U07, K_U08, K_U09 K_K02

Deepfake i bezpieczeństwo poznawcze (semestr 7): W ramach zajęć studenci zapoznają się z problematyką dezinformacji, manipulacji przekazem oraz zagrożeń dla bezpieczeństwa poznawczego jednostek, organizacji i państwa. Kurs obejmuje mechanizmy powstawania i rozpowszechniania fałszywych lub zmanipulowanych informacji, techniki wpływu informacyjnego, propagandę, polaryzację społeczną, podatność odbiorców na manipulację oraz rolę mediów społecznościowych i platform cyfrowych w kształtowaniu środowiska informacyjnego. Omawiane są również zagrożenia wynikające z rozwoju narzędzi generatywnej sztucznej inteligencji, w tym technologie deepfake, syntetyczne obrazy, głos i wideo, automatyzacja tworzenia treści, manipulacja kontekstem oraz trudności w ocenie autentyczności przekazów cyfrowych. Zajęcia rozwijają umiejętność krytycznej analizy komunikatów medialnych, rozpoznawania technik dezinformacyjnych, oceny wiarygodności źródeł, identyfikowania potencjalnych manipulacji cyfrowych oraz formułowania działań zwiększających odporność informacyjną i poznawczą.	K_W01 K_U01 K_K01, K_K03
Zarządzanie kryzysowe (semestr 7): W ramach zajęć studenci zapoznają się z podstawami zarządzania kryzysowego oraz jego znaczeniem dla bezpieczeństwa państwa, organizacji, infrastruktury krytycznej i cyberprzestrzeni. Kurs obejmuje pojęcia, struktury i procesy zarządzania kryzysowego, system zarządzania kryzysowego w Polsce, fazy zarządzania kryzysowego, rolę centrów zarządzania kryzysowego, monitorowanie zagrożeń, systemy wczesnego ostrzegania, postępowanie w sytuacji kryzysowej, odzyskiwanie po awarii oraz planowanie ciągłości działania. Omawiane są również współzależności między zagrożeniami w świecie fizycznym i cyfrowym, wpływ zakłóceń cyberbezpieczeństwa na funkcjonowanie ludności, instytucji i usług kluczowych oraz wykorzystanie technologii informacyjno-komunikacyjnych jako wsparcia procesów zarządzania kryzysowego. Zajęcia rozwijają umiejętność analizy sytuacji kryzysowej, identyfikowania jej skutków, proponowania działań ograniczających straty oraz współpracy z podmiotami odpowiedzialnymi za bezpieczeństwo i ciągłość działania.	K_W01 K_U01 K_K01, K_K03
Zarządzanie strategiczne w cyberbezpieczeństwie (semestr 7): W ramach zajęć studenci zapoznają się z problematyką strategicznego zarządzania cyberbezpieczeństwem w organizacjach, instytucjach publicznych oraz w systemie bezpieczeństwa państwa. Kurs obejmuje podstawowe pojęcia i modele zarządzania strategicznego, analizę otoczenia bezpieczeństwa, identyfikację celów strategicznych, planowanie działań długookresowych, budowanie polityk i programów cyberbezpieczeństwa oraz ocenę zdolności organizacji do ochrony zasobów informacyjnych i reagowania na zagrożenia. Omawiane są również zagadnienia zarządzania ryzykiem na poziomie strategicznym, ochrony infrastruktury krytycznej, ciągłości działania, odporności organizacyjnej, współpracy międzysektorowej, roli kierownictwa, komunikacji kryzysowej, zgodności z wymaganiami prawnymi i normatywnymi oraz monitorowania skuteczności przyjętej strategii. Zajęcia rozwijają umiejętność analizowania cyberbezpieczeństwa jako elementu zarządzania organizacją i bezpieczeństwa państwa, formułowania celów strategicznych, przygotowywania rekomendacji zarządczych oraz oceny konsekwencji decyzji podejmowanych w obszarze bezpieczeństwa cyfrowego.	K_W01 K_U01, K_U04 K_K01, K_K03

MODUŁ PRAKTYKI	EFEKTY KIERUNKOWE
Praktyka zawodowa: Bezpieczeństwo systemów i sieci teleinformatycznych (semestr 6) : Celem praktyki zawodowej na kierunku Cyberbezpieczeństwo jest utrwalenie wiedzy zdobytej przez studenta oraz rozwinięcie umiejętności niezbędnych do wykonywania zadań zawodowych związanych z bezpieczeństwem systemów i sieci teleinformatycznych. Praktyka umożliwia zastosowanie wiedzy teoretycznej w rzeczywistych warunkach pracy, weryfikację kompetencji wymaganych od absolwenta oraz rozwijanie umiejętności technicznych, organizacyjnych i analitycznych związanych z administracją i ochroną infrastruktury teleinformatycznej. Studenci mają możliwość poznania specyfiki pracy w zespołach odpowiedzialnych za bezpieczeństwo systemów informatycznych, administrację systemami i sieciami komputerowymi, monitorowanie infrastruktury, zarządzanie bezpieczeństwem informacji, obsługę incydentów oraz wdrażanie podstawowych procedur i mechanizmów ochrony systemów i danych. Praktyka pozwala również na zdobycie doświadczenia w zakresie konfiguracji i utrzymania środowisk informatycznych oraz stosowania narzędzi wspierających bezpieczeństwo infrastruktury cyfrowej. Praktyka jest powiązana z programem studiów, w szczególności z modułami dotyczącymi bezpieczeństwa systemów operacyjnych, bezpieczeństwa sieci komputerowych, kryptografii, bezpieczeństwa infrastruktury teleinformatycznej, technologii wykrywania i zapobiegania cyberatakom oraz podstaw zarządzania bezpieczeństwem informacji. W trakcie praktyki rozwijane są także kompetencje społeczne, między innymi poprzez pracę w zespołach projektowych, komunikację z użytkownikami i administratorami, udział w szkoleniach wewnętrznych oraz dokumentowanie wykonanych zadań zgodnie z wymaganiami organizacji. Praktyka odbywa się w przedsiębiorstwach, instytucjach lub organizacjach realizujących zadania związane z administracją i bezpieczeństwem systemów teleinformatycznych, utrzymaniem infrastruktury IT, monitorowaniem bezpieczeństwa, ochroną danych oraz reagowaniem na incydenty bezpieczeństwa. Prowadzona jest w języku obowiązującym w danym przedsiębiorstwie lub instytucji. Zakończeniem praktyki jest jej zaliczenie wraz z oceną.	K_W01, K_W02, K_W03, K_W07, K_W09, K_W12 K_U01, K_U03, K_U04, K_U11, K_U14, K_U15 K_K01, K_K02, K_K03, K_K04
Praktyka zawodowa: Bezpieczeństwo aplikacji i danych (semestr 6): Celem praktyki zawodowej na kierunku Cyberbezpieczeństwo jest utrwalenie wiedzy zdobytej przez studenta oraz rozwinięcie umiejętności niezbędnych do wykonywania zadań zawodowych związanych z bezpieczeństwem aplikacji oraz ochroną danych przetwarzanych w systemach informatycznych. Praktyka umożliwia zastosowanie wiedzy teoretycznej w rzeczywistych warunkach pracy, weryfikację kompetencji wymaganych od absolwenta oraz rozwijanie umiejętności technicznych, analitycznych i organizacyjnych związanych z bezpieczeństwem oprogramowania, ochroną danych i bezpieczeństwem informacji. Studenci mają możliwość poznania specyfiki pracy w zespołach odpowiedzialnych za bezpieczeństwo aplikacji internetowych i mobilnych, ochronę danych, bezpieczeństwo usług cyfrowych, testowanie bezpieczeństwa oraz wspieranie procesów związanych z utrzymaniem i rozwojem bezpiecznych środowisk informatycznych. Praktyka pozwala również na zdobycie doświadczenia w zakresie stosowania narzędzi wspierających ochronę aplikacji i danych oraz realizację podstawowych procedur bezpieczeństwa informacji. Praktyka jest powiązana z programem studiów, w szczególności z modułami dotyczącymi bezpieczeństwa aplikacji internetowych, ochrony danych, kryptografii, bezpieczeństwa usług cyfrowych, technologii wykrywania i zapobiegania cyberatakom oraz podstaw programowania i administracji systemami informatycznymi. W trakcie praktyki rozwijane są także kompetencje społeczne, między innymi poprzez pracę w zespołach projektowych, komunikację z użytkownikami i specjalistami IT, udział w szkoleniach wewnętrznych oraz dokumentowanie wykonanych zadań zgodnie z wymaganiami organizacji. Praktyka odbywa się w przedsiębiorstwach, instytucjach lub organizacjach realizujących zadania związane z bezpieczeństwem aplikacji, ochroną danych, rozwojem i utrzymaniem systemów informatycznych, bezpieczeństwem usług cyfrowych oraz wspieraniem procesów bezpieczeństwa informacji. Prowadzona jest w języku obowiązującym w danym przedsiębiorstwie lub instytucji. Zakończeniem praktyki jest jej zaliczenie wraz z oceną.	K_W01, K_W02, K_W05, K_W09, K_W12 K_U01, K_U02, K_U03, K_U11, K_U14, K_U15 K_K01, K_K02, K_K03, K_K04

MODUŁ DYPLOMOWY	EFEKTY KIERUNKOWE
Projekt inżynierski (semestr 7): W ramach zajęć studenci przygotowują się do kompleksowej realizacji projektu inżynierskiego, który stanowi praktyczne podsumowanie wiedzy i umiejętności zdobytych podczas studiów na kierunku Cyberbezpieczeństwo. Kurs ma formę seminarium projektowego i obejmuje pełny cykl życia rozwiązania informatycznego lub organizacyjno-technicznego związanego z bezpieczeństwem systemów informacyjnych, od analizy problemu i określenia wymagań, przez projektowanie architektury rozwiązania, dobór technologii i implementację, aż po testowanie, dokumentowanie oraz prezentację wyników. Studenci pracują zespołowo nad wybranym zagadnieniem praktycznym, tworząc działające oprogramowanie, usługę, konfigurację, procedurę, środowisko testowe, narzędzie analityczne lub inne rozwiązanie związane z cyberbezpieczeństwem. Dopuszcza się realizację projektów interdyscyplinarnych we współpracy ze studentami innych kierunków informatycznych, w szczególności informatyki lub inżynierii autonomicznych systemów cyfrowych, jeżeli zakres zadań realizowanych przez studentów kierunku Cyberbezpieczeństwo odpowiada efektom uczenia się i profilowi tego kierunku. Zajęcia rozwijają umiejętności planowania pracy projektowej, analizy ryzyka, podejmowania decyzji technologicznych, zarządzania zadaniami, współpracy w zespole oraz przygotowywania dokumentacji technicznej, użytkowej i projektowej. Kurs kładzie również nacisk na komunikację w zespole, prezentację rezultatów, krytyczną analizę decyzji projektowych oraz odpowiedzialne uwzględnianie wymagań bezpieczeństwa, prawa i etyki zawodowej. Realizacja projektu przygotowuje studentów do pracy zawodowej w rolach związanych z administracją systemami i sieciami, analizą bezpieczeństwa, testowaniem zabezpieczeń, monitorowaniem incydentów, projektowaniem rozwiązań ochronnych oraz wdrażaniem i utrzymaniem bezpiecznych systemów teleinformatycznych.	K_W06 K_U12, K_U14 K_K04

PLAN STUDIÓW – ZAŁĄCZNIK 3a

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
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		**41**	**15**	**0**	**0**	**0**	**0**	**15**	**71**	**0**	**6**	**2**	**3**	**0**	
Szkolenie BHK	A	4							4	z					
Szkolenie biblioteczne	A	2							2	z					
Ochrona własności intelektualnej	A							15	15	z	1				NP
Wykład z zakresu nauk humanistyczno-społecznych	F	15							15	z	2	0,6	1,4	0	NH/NS
Podstawy przedsiębiorczości	F	20	15						35	zo	3	1,4	1,6	0	EiF
MODUŁ PODSTAWOWY		**90**	**45**	**55**	**60**	**0**	**0**	**0**	**250**		**19**	**10**	**9**	**6**	
Wstęp do matematyki	B			30					30	zo	2	1,2	0,8	0	M
Matematyka dyskretna	B	20		25					45	zo	3	1,8	1,2	0	M
Teoretyczne podstawy informatyki	B	25	30						55	E	5	2,2	2,8	0	ITiT
Programowanie	B	30			60				90	zo /E	7	3,6	3,4	6	ITiT
Wstęp do cyberbezpieczeństwa	B	15	15						30	zo	2	1,2	0,8	0	ITiT
MODUŁ KIERUNKOWY		**15**	**15**	**0**	**0**	**0**	**0**	**0**	**30**		**2**	**1,2**	**0,8**	**0**	
Teoria bezpieczeństwa	C	15	15						30	zo	2	1,2	0,8	0	NoB
MODUŁ KURSÓW OBIERALNYCH		**10**	**0**	**0**	**30**	**0**	**0**	**0**	**40**		**3**	**1,6**	**1,4**	**2**	
Języki skryptowe	E	10			30				40	zo	3	1,6	1,4	2	ITiT
Programowanie funkcyjne (Python)	E	10			30				40	zo	3	1,6	1,4	2	ITiT
		156	75	55	90	0	0	15	391		30	14,8	14,2	8	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
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**	**40**	**0**	**0**	**0**	**0**	**40**		**3**	**1,6**	**1,4**	**3**	
Język obcy B2 - 1	A			40					40	z	3	1,6	1,4	3	J
MODUŁ PODSTAWOWY		**80**	**0**	**40**	**105**	**0**	**0**	**0**	**225**		**18**	**9**	**9**	**9**	
Matematyka 1	B	20		40					60	E	5	2,4	2,6	0	M
Organizacja i architektura komputerów	B	20			30				50	zo	4	2	2	3	ITiT
Algorytmy i struktury danych	B	30			45				75	E	6	3	3	4	ITiT
Wprowadzenie do sieci komputerowych	B	10			30				40	zo	3	1,6	1,4	2	ITiT
MODUŁ KIERUNKOWY		**20**	**0**	**0**	**60**	**0**	**0**	**0**	**80**		**6**	**3,2**	**2,8**	**5**	
Programowanie obiektowe	C	20			30				50	zo	4	2	2	3	ITiT
Podstawy systemów kontroli wersji i pracy zespołowej w IT	C				30				30	zo	2	1,2	0,8	2	ITiT
MODUŁ KURSÓW OBIERALNYCH		**10**	**0**	**0**	**30**	**0**	**0**	**0**	**40**		**3**	**1,6**	**1,4**	**2**	
Programowanie systemowe (C lub C++)	E	10			30				40	zo	3	1,6	1,4	2	ITiT
Języki hipertekstowe i tworzenie stron WWW	E	10			30				40	zo	3	1,6	1,4	2	ITiT
		110	0	80	195	0	0	0	385		30	15,4	14,6	19	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
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 OGÓLNOUCZELNIANY		**0**	**30**	**40**	**0**	**0**	**0**	**0**	**70**		**3**	**1,6**	**1,4**	**3**	
Język obcy B2 - 2	A			40					40	z	3	1,6	1,4	3	J
Kultura fizyczna	A		30						30	z	0	0	0	0	NoKF
MODUŁ PODSTAWOWY		**40**	**0**	**55**	**0**	**0**	**0**	**0**	**95**		**7**	**3,8**	**3,2**	**0**	
Matematyka 2	B	25		30					55	E	4	2,2	1,8	0	M
Podstawy kodowania	B	15		25					40	zo	3	1,6	1,4	0	ITiT
MODUŁ KIERUNKOWY		**60**	**0**	**0**	**115**	**0**	**0**	**0**	**175**		**14**	**7**	**7**	**10**	
Systemy operacyjne	C	20			30				50	zo	4	2	2	3	ITiT
Konfiguracja i zarządzanie sieciami komputerowymi	C	30			30				60	E	5	2,4	2,6	4	ITiT
Wprowadzenie do technologii chmury	C	10			30				40	zo	3	1,6	1,4	2	ITiT
Standaryzacja systemów cyberbezpieczeństwa	C				25				25	zo	2	1	1	1	ITiT
MODUŁ KURSÓW OBIERALNYCH		**20**	**0**	**0**	**60**	**0**	**0**	**0**	**80**		**6**	**3,2**	**2,8**	**4**	
Technologie DevSecOps	E	10			30				40	zo	3	1,6	1,4	2	ITiT
Programowanie niskopoziomowe	E	10			30				40	zo	3	1,6	1,4	2	ITiT
Programowanie aplikacji internetowych (Java)	E	10			30				40	zo	3	1,6	1,4	2	ITiT
		120	30	95	175	0	0	0	420		30	15,6	14,4	17	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
Nabór: 2026/2027

Semestr 4

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**	**30**	**30**	**0**	**0**	**0**	**0**	**60**		**4**	**1,2**	**2,8**	**4**	
Język obcy B2 - 3	A			30					30	E	4	1,2	2,8	4	J
Kultura fizyczna	A		30						30	z	0	0	0	0	NoKF
MODUŁ PODSTAWOWY		**20**	**0**	**0**	**35**	**0**	**0**	**0**	**55**		**4**	**2,2**	**1,8**	**3**	
Fizyka i elektronika	B	20			35				55	zo	4	2,2	1,8	3	NF
MODUŁ KIERUNKOWY		**85**	**15**	**0**	**110**	**0**	**0**	**0**	**210**		**15**	**8,4**	**6,6**	**10,5**	
Podstawy sztucznej inteligencji	C	30			30				60	E	5	2,4	2,6	4	ITiT
Bazy danych	C	15			30				45	zo	3	1,8	1,2	2	ITiT
Bezpieczeństwo systemów operacyjnych	C	15			20				35	zo	2	1,4	0,6	2	ITiT
Bezpieczeństwo sieci komputerowych	C	10			30				40	zo	3	1,6	1,4	2,5	ITiT
Militarny wymiar cyberbezpieczeństwa	C	15	15						30	z	2	1,2	0,8	0	NoB
MODUŁ KURSÓW OBIERALNYCH		**30**	**0**	**0**	**50**	**0**	**0**	**0**	**80**		**6**	**3,2**	**2,8**	**4**	
Teoria zarządzania ryzykiem cyberbezpieczeństwa	E	15			25				40	zo	3	1,6	1,4	2	ITiT
Przetwarzanie sygnałów	E	15			25				40	zo	3	1,6	1,4	2	ITiT
Bezpieczeństwo technologii chmurowych	E	15			25				40	zo	3	1,6	1,4	2	ITiT
		135	45	30	195	0	0	0	405		29	15	14	21,5	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
Nabór: 2026/2027

Semestr 5

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		**95**	**70**	**0**	**120**	**0**	**0**	**0**	**285**		**22**	**11,4**	**10,6**	**11,5**	
Bezpieczeństwo baz danych	C				30				30	zo	2	1,2	0,8	2	ITiT
Kryptografia	C	20	30						50	E	4	2	2	2,5	ITiT
Bezpieczeństwo aplikacji internetowych	C	10			30				40	zo	3	1,6	1,4	2	ITiT
Inżynieria odwrotna	C	10			30				40	zo	3	1,6	1,4	2	ITiT
Zarządzanie projektami cyberbezpieczeństwa	C		10		10				20	zo	2	0,8	1,2	1	ITiT
Metody zbierania informacji	C	20			20				40	zo	3	1,6	1,4	2	ITiT
Wojny informacyjne	C	15	15						30	z	2	1,2	0,8	0	NoB
Podstawy prawne cyberbezpieczeństwa	F	20	15						35	E	3	1,4	1,6	0	NoB
MODUŁ KURSÓW OBIERALNYCH		**30**	**0**	**0**	**90**	**0**	**0**	**0**	**120**		**9**	**4,8**	**4,2**	**6**	
Metody i narzędzia zabezpieczania aplikacji AI	E	10			30				40	zo	3	1,6	1,4	2	ITiT
Bezpieczeństwo systemów AI i LLM	E	10			30				40	zo	3	1,6	1,4	2	ITiT
Bezpieczeństwo systemów elektronicznych	E	10			30				40	zo	3	1,6	1,4	2	ITiT
AI w reagowaniu na incydenty w kryminalistyce cyfrowej	E	10			30				40	zo	3	1,6	1,4	2	ITiT
		125	70	0	210	0	0	0	405		31	16,2	14,8	17,5	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
Nabór: 2026/2027

Semestr 6

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 PRAKTYKI[2]		**0**	**0**	**0**	**0**	**0**	**960**	**0**	**960**		**30**	**0**	**0**	**30**	
Praktyka zawodowa	E/H						960		960	zo	30			30	
		0	0	0	0	0	960	0	960		30	0	0	30	

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
Nabór: 2026/2027

Semestr 7

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		**60**	**0**	**0**	**75**	**50**	**0**	**0**	**185**		**16**	**7,4**	**8,6**	**13**	
Technologie decentralizacji danych (Blockchain)	C	20			30				50	zo	4	2	2	3	ITiT
Technologie wykrywania i zapobiegania cyberatakom	C	20			25				45	zo	4	1,8	2,2	3	ITiT
Metodyki testów penetracyjnych	C	20			20				40	zo	3	1,6	1,4	2	ITiT
Projekt inżynierski	C					50			50	zo	5	2	3	5	ITiT
MODUŁ KURSÓW OBIERALNYCH		**40**	**40**	**0**	**0**	**0**	**0**	**0**	**80**		**6**	**3,2**	**2,8**	**0**	
Deepfake i bezpieczeństwo poznawcze	E	20	20						40	z	3	1,6	1,4	0	NoB
Zarządzanie kryzysowe	E	20	20						40	z	3	1,6	1,4	0	NoB
Zarządzanie strategiczne w cyberbezpieczeństwie	E	20	20						40	z	3	1,6	1,4	0	NoB
MODUŁ DYPLOMOWY		**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**8**	**0**	**0**	**0**	
Egzamin inżynierski	A										8				ITiT
		100	40	0	75	50	0	0	265		30	10,6	11,4	13	

1. Grupa przedmiotów (A-obligatoryjne, B-podstawowe, C-kierunkowe, D-specjalnościowe, E-obieralne, F-humanistyczno-społeczne, G-języki obce, H-praktyki)
2. Praktyki - 6 miesięcy praktyki ciągłej (960h lekcyjnych = 720h zegarowych)

Plan studiów: CYBERBEZPIECZEŃSTWO

Profil: PRAKTYCZNY
Stopień: PIERWSZY
Forma: STACJONARNE
Nabór: 2026/2027

PODSTAWOWE INFORMACJE O PROGRAMIE KSZTAŁCENIA I KIERUNKU STUDIÓW	CYBERBEZPIECZEŃSTWO
Liczba semestrów	7
Łączna liczba godzin pracy studenta w planie studiów	2271
Łączna liczba punktów ECTS konieczna do ukończenia studiów	210
Łączna liczba godzin przeznaczonych na praktyki zawodowe	960
Łączna liczba punktów ECTS przeznaczonych na praktyki zawodowe	30
Łączna liczba punktów ECTS przeznaczonych na pracę dyplomową	8
Procentowy udział w ramach zajęć w bezpośrednim udziale NA	50,9%
Łączna liczba punktów ECTS powiązanych z działalnością naukową	169
Łączna liczba punktów ECTS powiązanych z działalnością naukową w dyscyplinie **ITiT**	131
Łączna liczba punktów ECTS kształtujących umiejętności praktyczne	126
Łączna liczba punktów ECTS przyporządkowanych kursom z zakresu nauk human.-społ. (F)	8
Łączna liczba godzin zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	746
Łączna liczba punktów ECTS przyporządkowanych kursom do wyboru	63
Łączna liczba punktów ECTS - procentowy udział kursów do wyboru	30,0%
Łączna liczba godzin zajęć z języków obcych	110
Łączna liczba punktów ECTS przypisana zajęciom z języków obcych	10

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

Kraków, dn. 9.06.2026 r.

Uchwała nr 18/IBiI/26
Rady Instytutu Bezpieczeństwa i Informatyki
Uniwersytetu Komisji Edukacji Narodowej w Krakowie
z dnia 9 czerwca 2026 r.

Rada Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie podjęła uchwałę w sprawie zatwierdzenia programów i planów studiów dla kierunków:
1) Informatyka - studiów pierwszego stopnia o profilu praktycznym (studia stacjonarne i niestacjonarne),
2) Cyberbezpieczeństwo - studiów pierwszego stopnia o profilu praktycznym (studia stacjonarne i niestacjonarne), edycji rozpoczynających się w roku akademickim 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 10.06.2026 r.

OPINIA nr 5/RJK/2026

Rady Jakości Kształcenia dla kierunku

INFORMATYKA i CYBERBEZPIECZEŃSTWO

dotyczy

programów i planów studiów

kierunków Informatyka oraz Cyberbezpieczeństwo

studia I stopnia stacjonarne i niestacjonarne

cykl 2026/27

Instytutowa Rada Jakości Kształcenia pozytywnie opiniuje programy i plany studiów:

1. Informatyka 1 stopnia (stacjonarne i niestacjonarne) nabór 2026-27
2. Cyberbezpieczeństwo 1 stopnia (stacjonarne i niestacjonarne) nabór 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, 11.06.2026

Opinia Instytutowej Rady Samorządu Studentów 4-IRSS-26
Instytutu Bezpieczeństwa i Informatyki
Uniwersytetu Komisji Edukacji Narodowej w Krakowie

w sprawie programu i planu studiów dla kierunku Cyberbezpieczeństwo (studia I stopnia) realizowanych w formie stacjonarnej.

Na podstawie dostarczonych źródeł Instytutowa Rada Samorządu Studentów Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie dokonała oceny programu i planu studiów dla kierunku Cyberbezpieczeństwo I stopnia (studia stacjonarne) 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

Instytutowa Rada Samorządu Studentów
Uniwersytetu Komisji Edukacji Narodowej
w Krakowie

ul. Podchorążych 2, pok. 270
30-084 Kraków
www.samorzad.uken.krakow.pl

Biuro Samorządu Studentów
tel. 12 662 61 19
samorzad@up.krakow.pl