

CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

PROGRAM STUDIÓW WYŻSZYCH ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM 2024/2025

data zatwierdzenia przez Radę Instytutu

pieczęć i podpis Dyrektora Instytutu

.....

Studia wyższe na kierunku	CYBERBEZPIECZEŃSTWO
Dziedzina/y	Nauki inżynieryjno-techniczne Nauki społeczne
Dyscyplina wiodąca (% udział)	Informatyka techniczna i telekomunikacja (80%)
Pozostałe dyscypliny (% udział)	Nauki o bezpieczeństwie (20%)
Poziom	pierwszy (studia inżynierskie I stopnia)
Profil	praktyczny
Forma prowadzenia	studia niestacjonarne
Specjalności	–
Punkty ECTS	210
Czas realizacji (liczba semestrów)	7 semestrów
Uzyskiwany tytuł zawodowy	inżynier
Warunki przyjęcia na studia	Kryteria przyjęć na studia dla kandydatów z „nową maturą”: Dla nowej matury: 1% = 1 punkt. O miejscu na liście rankingowej decyduje większa z liczb: • wynik (w punktach) egzaminu maturalnego z matematyki – poziom podstawowy, część pisemna • 2 x wynik (w punktach) egzaminu maturalnego z matematyki lub informatyki – poziom rozszerzony, część pisemna. Kryteria przyjęć na studia dla kandydatów ze „starą maturą”: o miejscu na liście rankingowej decyduje większa z liczb: • przeliczona na punkty (według podanego poniżej przelicznika) ocena z pisemnego egzaminu dojrzałości z matematyki lub informatyki, • przeliczona na punkty (według podanego poniżej przelicznika) ocena z ustnego egzaminu dojrzałości z matematyki lub informatyki, • 0,75 x przeliczona na punkty (według podanego poniżej przelicznika) ocena z egzaminu dojrzałości z jednego z przedmiotów: fizyka, chemia, – część pisemna. Przelicznik ocen ze świadectw starej matury na punkty:

CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

	Dopuszczający - 30 punktów Dostateczny - 50 punktów Dobry - 70 punktów Bardzo dobry - 90 punktów Celujący - 100 punktów UWAGA: Laureaci i finaliści olimpiad stopnia centralnego będą przyjmowani na studia według obowiązującej w czasie postępowania kwalifikacyjnego Uchwały Senatu Uniwersytetu Komisji Edukacji Narodowej w Krakowie.
--	---

Efekty uczenia się

Symbol efektu kierunkowego	Kierunkowe efekty uczenia się	Odniesienie do efektów uczenia się zgodnych z Polską Ramą Kwalifikacji	
		Symbol charakterystyk uniwersalnych I stopnia ¹	Symbol charakterystyk II stopnia ²
WIEDZA: ABSOLWENT zna i rozumie:			
K_W01	w zaawansowanym stopniu fakty i teorie stanowiące wiedzę z przedmiotów ścisłych, zwłaszcza matematyki i fizyki, niezbędną do opisu i analizy działania sieci komputerowych i urządzeń sieciowych, a także innych urządzeń zakresu technik komputerowych oraz algorytmów ich funkcjonowania	P6U_W	P6S_WG
K_W02	w zaawansowanym stopniu fakty i teorie stanowiące wiedzę w zakresie zabezpieczania architektury systemów komputerowych, systemów operacyjnych i urządzeń sieciowych.	P6U_W	P6S_WG
K_W03	elementarne algorytmy, języki i techniki programowania oraz zasady projektowania systemów baz danych w kontekście wymagań bezpieczeństwa	P6U_W	P6S_WG
K_W04	zagadnienia dotyczące systemów informatycznych i sieci komputerowych oraz zasady ich organizacji i administracji	P6U_W	P6S_WG
K_W05	zasady działania podstawowych narzędzi kryptograficznych w kontekście zapewnienia optymalnego zabezpieczenia struktur lokalnych i sieciowych	P6U_W	P6S_WG
K_W06	zasady działania aplikacji i usług elektronicznych w Internecie i w sieciach lokalnych ze szczególnym uwzględnieniem aspektów bezpieczeństwa	P6U_W	P6S_WG
K_W07	w zaawansowanym stopniu pojęcia, struktury i procesy z zakresu cyberbezpieczeństwa (w tym zagrożenia i szanse wynikające z funkcjonowania w świecie cyfrowym wpływające na współczesne państwa, społeczeństwa, podmioty prywatne), jak również przykłady je ilustrujące oraz zależności występujące w obrębie wiedzy dotyczącej bezpieczeństwa w cyberprzestrzeni	P6U_W	P6S_WG
K_W08	zna podstawy analizy matematycznej i algebry, matematyki dyskretnej oraz metod numerycznych w zakresie umożliwiającym opis oraz modelowanie problemów występujących w systemach komputerowych	P6U_W	P6S_WG

¹ Zgodnie z załącznikiem do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2016, poz.64).

² Zgodnie z załącznikiem 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 (Dz. U. z 2018 r., poz. 2218).

CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

K_W09	zna podstawy logiki matematycznej, rachunek zbiorów, rachunek prawdopodobieństwa w zakresie umożliwiającym rozwiązywanie problemów algorytmicznych	P6U_W	P6S_WG
K_W10	w zaawansowanym stopniu prawne, techniczne, ekonomiczno-społeczne i inne uwarunkowania cyberbezpieczeństwa oraz polityki przeciwdziałania przestępczości w cyberprzestrzeni (w tym zaawansowane zasady tworzenia i rozwoju polityki bezpieczeństwa informacyjnego)	P6U_W	P6S_WK
K_W11	istotę człowieka jako podmiotu kształtującego współczesne struktury i procesy w środowisku bezpieczeństwa narodowego i międzynarodowego oraz cyberbezpieczeństwa, generującym szanse i zagrożenia dla jego przyszłości	P6U_W	P6S_WK
K_W12	główne tendencje rozwojowe, najistotniejsze nowe osiągnięcia oraz dylematy etyczne w obszarze cyberbezpieczeństwa	P6U_W	P6S_WK
UMIEJĘTNOŚCI ABSOLWENT potrafi:			
K_U01	korzystać z nowoczesnych narzędzi IT w zakresie planowania, budowania i eksploatacji sieci komputerowych o lokalnym i rozszerzonym zasięgu w oparciu o zasady bezpieczeństwa funkcjonowania tych struktur	P6U_U	P6S_UW
K_U02	wykorzystywać nowoczesne narzędzia technologii informacyjno-komunikacyjnych w zakresie obsługi (instalacji, konfiguracji i eksploatacji) systemów operacyjnych	P6U_U	P6S_UW
K_U03	używać dedykowanych środowisk programistycznych wraz z wybranymi bibliotekami w celu efektywnego i bezpiecznego tworzenia aplikacji desktopowych, mobilnych czy internetowych	P6U_U	P6S_UW
K_U04	konstruować algorytmy i pisać pojedyncze aplikacje oraz większe projekty programistyczne, w oparciu o języki programowania niskiego i wysokiego poziomu z uwzględnieniem zasad bezpieczeństwa	P6U_U	P6S_UW
K_U05	pracować indywidualnie lub w zespole (m.in. opracować dokumentację, przedstawić prezentację i prowadzić dyskusję na temat zadania, projektu lub zagadnień w szczególności zw. z cyberbezpieczeństwem, również w jęz. obcym) oraz planować pracę, a także komunikować się przy użyciu technik właściwych dla branży IT	P6U_U	P6S_UO
K_U06	zaplanować i przeprowadzać testy, eksperymenty i badania z dziedziny telekomunikacji i informatyki, w szczególności związane z cyberbezpieczeństwem	P6U_U	P6S_UO
K_U07	analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania	P6U_U	P6S_UW
K_U08	konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych	P6U_U	P6S_UW
K_U09	dokonać analizy pod kątem bezpieczeństwa struktur krytycznych z zakresu sieci komputerowych i systemów operacyjnych	P6U_U	P6S_UW
K_U10	formułować i rozwiązywać złożone, typowe i nietypowe problemy zw. z kryptografią dobierając odpowiednie źródła informacji (również w języku obcym) oraz krytycznie je analizując i syntetyzując, a także wybierając stosowne narzędzia programistyczne, sprzętowe i sieciowe	P6U_U	P6S_UW
K_U11	prawidłowo dostrzec, ocenić i interpretować zjawiska w zakresie cyberbezpieczeństwa oraz rozwoju nowych	P6U_U	P6S_UW

CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

	technologii w ujęciu historycznym, politycznym, społecznym, gospodarczym, militarnym, etycznym, prawnym (w tym w zakresie ochrony własności intelektualnej).		
K_U12	posługiwać się co najmniej jednym językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego oraz terminologią w zakresie cyberbezpieczeństwa	P6U_U	P6S_UK
K_U13	stosować definicje i twierdzenia pozwalające na opisywanie problemów algorytmicznych za pomocą języka i formalizmu matematycznego.	P6U_U	P6S_UK
K_U14	planować i realizować proces samokształcenia i rozwój zawodowy w branży IT, w szczególności w sektorze cyberbezpieczeństwa.	P6U_U	P6S_UU
KOMPETENCJE SPOŁECZNE ABSOLWENT jest gotów do:			
K_K01	inicjowania działań na rzecz współdziałania z innymi osobami w ramach prac zespołowych i podejmowania różnych wiodących ról w interdyscyplinarnych zespołach zajmujących się analizowaniem cyberbezpieczeństwa oraz myślenia i działania w sposób przedsiębiorczy	P6U_K	P6S_KO
K_K02	krytycznej oceny poziomu swojej wiedzy oraz ciągłego dokształcania się i konsultacji z innymi ekspertami z branży IT w szczególności związanej z cyberbezpieczeństwem, a także planowania własnego rozwoju zawodowego	P6U_K	P6S_KK
K_K03	respektowania zasad etycznych i prawnych w cyberprzestrzeni oraz zobowiązań płynących z wykonywanego zawodu (w tym poszanowania prawa własności intelektualnej)	P6U_K	P6S_KR
K_K04	uznawania znaczenia tworzenia i wdrażania rozwiązań z obszaru cyberbezpieczeństwa w podnoszeniu jakości życia na świecie (na poziomie jednostki oraz zbiorowości)	P6U_K	P6S_KO
K_K05	inicjowania działań w złożonym ekosystemie podmiotów związanych z zapewnianiem cyberbezpieczeństwa – zarówno z punktu widzenia sektora prywatnego jak i publicznego	P6U_K	P6S_KO

CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

Sylwetka absolwenta	Absolwent kierunku <i>Cyberbezpieczeństwo</i> uczestnicząc w procesie dydaktycznym realizowanym za pomocą innowacyjnych metod kształcenia posiada interdyscyplinarną wiedzę z zakresu nauk inżynieryjno-technicznych, ścisłych i przyrodniczych oraz społecznych w zakresie cyberbezpieczeństwa, jak również rozumie i potrafi efektywnie analizować procesy zachodzące w środowisku cyfrowym w biznesie i podmiotach publicznych oraz osób fizycznych. Ma wiedzę z zakresu: • dostępnych rozwiązań w obszarze zabezpieczeń aplikacji, systemów i sieci komputerowych • projektowania, tworzenia, konfiguracji i wykorzystania narzędzi oraz technologii związanych z bezpieczeństwem systemów oraz sieci komputerowych (w celu zabezpieczania ich funkcjonowania w instytucjach publicznych oraz u wszelkiego rodzaju podmiotów prowadzących działalność gospodarczą) • nowoczesnych metod cyberbezpieczeństwa (kryptografii i sztucznej inteligencji) • działania aplikacji i usług elektronicznych w Internecie (a także w sieciach o mniejszym zasięgu, w tym lokalnych). Ponadto zna zagrożenia cyberprzestrzeni i świata wirtualnego, w tym m.in.: • aspekty prawne, kryminologiczne i techniczne cyberprzestępczości • patologiczne formy korzystania z mediów i cyberprzemocy • zagrożenia bezpieczeństwa informacyjnego. Absolwent kierunku cyberbezpieczeństwo posiada umiejętności i kompetencje w zakresie: • wykorzystania nowoczesnych narzędzi w ramach sieci komputerowych, systemów operacyjnych technik tworzenia aplikacji • pracy w różnego typu środowiskach programistycznych • doboru, konfiguracji i eksploatacji specjalistycznego sprzętu sieciowego (szczególnie w zastosowaniach dotyczących projektowania i integracji systemów bezpieczeństwa) • zabezpieczania systemów komputerowych przed atakami oraz dokonywania analizy struktur wrażliwych • kształtowania kultury bezpieczeństwa współczesnego człowieka, minimalizacji zagrożeń w celu zapewnienia ochrony danych osobowych, finansów, tożsamości i prywatności, zwalczania cyberprzestępczości, jak również zapobiegania patologiom cyfrowym.
Uzyskiwane kwalifikacje oraz uprawnienia zawodowe	Absolwenci tego kierunku studiów mogą podjąć pracę w obszarach związanych z bezpieczeństwem w cyberprzestrzeni (sektor prywatny/publiczny), w tym: • podmiotach tworzących krajowy system cyberbezpieczeństwa (np. w policyjnych wydziałach do walki z cyberprzestępczością, wojskach obrony cyberprzestrzeni), jak również jako eksperci działów IT ds. bezpieczeństwa m.in. jako: • administratorzy sieci komputerowych • specjaliści ds. bezpieczeństwa • analitycy i konsultanci ds. cyberbezpieczeństwa • inżynierowie bezpieczeństwa • pentesterzy • Security Software Developerzy – programiści z wiedzą nt. cyberbezpieczeństwa, a także jako: • edukatorzy kompetencji cyfrowych • pracownicy instytucji publicznych odpowiedzialni za cyberbezpieczeństwo oraz szkolenia w tym obszarze • pracownicy organizacji typu fact-checkingowych.
Dostęp do dalszych studiów	Absolwenci studiów I stopnia uzyskują przygotowanie do pracy zawodowej, a także możliwość kontynuowania kształcenia na studiach II stopnia na kierunku Informatyka ze specjalnością cyberbezpieczeństwo, jak również pokrewnych kierunkach studiów oraz na studiach podyplomowych.

Jednostka badawczo-dydaktyczna właściwa merytorycznie dla tych studiów

Instytut Bezpieczeństwa i Informatyki

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr I

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Wstęp do matematyki		30						30	zo	3
Matematyka dyskretna	15	25						40	zo	4
Teoretyczne podstawy informatyki	15	20						35	zo	4
Programowanie*	20			40				60	zo /E	7
Wstęp do cyberbezpieczeństwa	10	10						20	zo	2
Podstawy przedsiębiorczości	15							15	zo	3
Teoria bezpieczeństwa	10	10						20	z	2
Ochrona własności intelektualnej							15	15	z	1
	85	95		40			15	235	1	26

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Języki skryptowe	6			20				26	zo	2
Programowanie funkcyjne (Python)										
Wykład z zakresu nauk humanistycznych lub społecznych	10							10	z	2
	16			20				36		4

Pozostałe zajęcia

rodzaj zajęć	godz.	forma zaliczenia	punkty ECTS
Szkolenie biblioteczne (e-learning)	2	z	0
Szkolenie BHK (e-learning)	4	z	0

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr II

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Matematyka 1	20	30						50	E	5
Algorytmy i struktury danych	20			20				40	zo	5
Organizacja i architektura komputerów	15			20				35	zo	5
Wprowadzenie do sieci komputerowych	6			20				26	zo	3
Języki i narzędzia programowania obiektowego				20				20	zo	2
Standaryzacja systemów cyberbezpieczeństwa		15						15	zo	2
Środowisko cyberbezpieczeństwa	15	10						25	E	3
	76	55		80				211	2	25

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Programowanie systemowe (C lub C++)				15				15	zo	2
Języki hipertekstowe i tworzenie stron WWW										
Język obcy B2 - 1			30					30	z	3
			30	15				45		5

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr III

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Matematyka 2	20	30						50	E	5
Systemy operacyjne	15			20				35	zo	4
Teoria informacji i kodowania	10			10				20	zo	3
Programowanie aplikacji internetowych (Java)	15			20				35	E	5
Konfiguracja i zarządzanie sieciami komputerowymi	15			20				35	zo	4
Nowe technologie w cyberprzestrzeni	6	10						16	z	2
Ochrona danych osobowych		10						10	z	1
	81	50		70				201	2	24

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Język obcy B2 - 2			30					30	z	3
Technologie DevOps	6			20				26	zo	3
Wprowadzeniedo technologii chmury										
	6		30	20				56		6

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr IV

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Programowanie niskopoziomowe				20				20	zo	3
Bezpieczeństwo systemów operacyjnych	10			10				20	zo	3
Bazy danych	10			15				25	zo	3
Inżynieria odwrotna				20				20	zo	2
Bezpieczeństwo sieci komputerowych	6			20				26	zo	3
Fizyka i elektronika	15			25				40	zo	4
Zarządzanie kryzysowe w cyberbezpieczeństwie	10	10						20	E	4
Biały wywiad		10						10	z	2
	51	20		110				181	1	24

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Język obcy B2 - 3			30					30	E	4
Manipulacja informacją		15						15	z	2
Kultura informacyjna w cyberbezpieczeństwie										
		15	30					45	1	6

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr V

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Bezpieczeństwo baz danych				20				20	zo	3
Kryptografia	15			20				35	E	4
Bezpieczeństwo systemów elektronicznych	6			15				21	zo	3
Podstawy prawne cyberbezpieczeństwa	15	10						25	E	4
Zarządzanie strategiczne w cyberbezpieczeństwie	10	15						25	E	4
	46	25		55				126	3	18

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Metody zbierania informacji	6			10				16	zo	2
Teoria zarządzania ryzykiem cyberbezpieczeństwa										
	6			10				16		2

Praktyki

nazwa praktyki	godz.	tyg.	forma zaliczenia	punkty ECTS
PRAKTYKA ZAWODOWA w instytucjach/firmach realizujących projekty informatyczne i z zakresu cyberbezpieczeństwa, dobranych pod kątem realizowanego kierunku.	240		z	10
Termin: praktyka nieciągła w trakcie całego semestru	240			10

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr VI

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Bezpieczeństwo aplikacji internetowych				20				20	zo	3
Technologie decentralizacji danych (Blockchain)	10			20				30	zo	4
Technologie wykrywania i zapobiegania cyberatakam	10			20				30	zo	3
Podstawy sztucznej inteligencji	6			20				26	zo	3
Militarny wymiar cyberbezpieczeństwa	15	10						25	z	2
Wojny informacyjne	10	10						20	z	2
	51	20		80				151		17

Kursy do wyboru

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Analiza malware	6			10				16	zo	2
Bezpieczeństwo technologii chmurowych										
	6			10				16		2

Praktyki

nazwa praktyki	godz.	tyg.	forma zaliczenia	punkty ECTS
PRAKTYKA ZAWODOWA w instytucjach/firmach realizujących projekty informatyczne i z zakresu cyberbezpieczeństwa, dobranych pod kątem realizowanego kierunku. Termin: praktyka nieciągła w trakcie całego semestru	240		z	10
	240			10

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2024-2028

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2024/2025

Semestr VII

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Metodyki testów penetracyjnych	10			10				20	zo	3
Zarządzanie projektami cyberbezpieczeństwa		6		6				12	zo	2
	10	6		16				32		5

Kursy do wyboru

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Systemy i narzędzia autentyfikacji	6			20				26	zo	3
Bezpieczeństwo handlu elektronicznego, bankowości i systemów płatności										
Projekt inżynierski**					30			30	zo	5
	6			20	30			56		8

Praktyki

nazwa praktyki	godz.	tyg.	forma zaliczenia	punkty ECTS
PRAKTYKA ZAWODOWA w instytucjach/firmach realizujących projekty informatyczne i z zakresu cyberbezpieczeństwa, dobranych pod kątem realizowanego kierunku. Termin: praktyka nieciągła w trakcie całego semestru	240		zo	10
	240			10

Egzamin dyplomowy inżynierski

Tematyka	ECTS
Egzamin inżynierski jest pisemnym i ustnym sprawdzianem potwierdzającym osiągnięcie wybranych efektów kształcenia w zakresie wiedzy i umiejętności, realizowanych w ramach studiów. Zakres egzaminu inżynierskiego obejmuje treści przedmiotów z grupy zajęć kierunkowych.	8

EN - kurs prowadzony w języku angielskim

*Kurs Programowanie kończy się zaliczeniem z oceną z ćwiczeń oraz egzaminem,

**Kurs obowiązkowy, którego tematyka jest do wyboru



Uniwersytet Komisji
Edukacji Narodowej
w Krakowie

INSTYTUT BEZPIECZEŃSTWA I INFORMATYKI

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

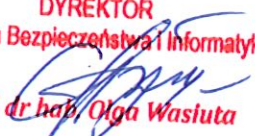
tel. 12 662 7845
e-mail: ii@uken.krakow.pl

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

Kraków, dn. 12.09.2025 r.

Uchwała nr 12/IBiI/25 Rady Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie z dnia 20 września 2025 r.

Rada Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie podjęła uchwałę w sprawie zatwierdzenia korekt w planach studiów na kierunkach Informatyka i Cyberbezpieczeństwo - studiów pierwszego stopnia o profilu praktycznym (studia stacjonarne i niestacjonarne). Korekty obowiązują od roku akademickiego 2025/26.

DYREKTOR
Instytutu Bezpieczeństwa i Informatyki

prof. dr hab. Olga Wasłuta

**Korekty w planach studiów 1-stopnia
kierunku Informatyka, Cyberbezpieczeństwo
od roku akademickiego 2025/2026**

Załącznik do UCHWAŁY
12/13.1/2025

Kierunek INFORMATYKA

PLAN STUDIÓW INŻYNIERSKICH 1-go stopnia 2022-2026

STUDIA STACJONARNE, STUDIA NIESTACJONARNE

semestr V

- 1) Kurs – Kryptografia – zmiana formy zaliczenia z egzaminu (E) na zaliczenie z oceną (zo); zmiana liczby godzin wykładu na studiach stacjonarnych z 25h na 20h, na studiach niestacjonarnych z 10h na 15h; zmiana liczby godzin ćwiczeń laboratoryjnych na studiach niestacjonarnych z 15h do 10h.

semestr VII

- 2) Kurs – Praktyczne zastosowania sztucznej inteligencji – zmniejszenie liczby godzin laboratoryjnych na studiach stacjonarnych z 40h na 30h, na studiach niestacjonarnych z 30h na 20h
- 3) Kurs – Inżynieria i analiza danych – zmniejszenie liczby godzin laboratoryjnych na studiach stacjonarnych z 45h na 30h.

Kierunek INFORMATYKA

PLAN STUDIÓW INŻYNIERSKICH 1-go stopnia 2023-2027

STUDIA STACJONARNE, STUDIA NIESTACJONARNE

semestr V

- 1) Kurs – Inżynieria oprogramowania – usunięcie z planu studiów.
- 2) Kurs - Bazy danych w aplikacjach internetowych – zmiana formy zaliczenia z zaliczenia z oceną (zo) na egzamin (E) oraz zwiększenie liczby punktów ECTS z 4 do 5.
- 3) Kurs - Systemy czasu rzeczywistego – zwiększenie liczby punktów ECTS z 2 do 3.
- 4) Kurs - Technologie DevOps – zmiana formy zaliczenia kursu z zaliczenia z oceną (zo) na egzamin (E); zwiększenie liczby punktów ECTS z 4 do 5; na studiach niestacjonarnych zmniejszenie liczby godzin wykładu z 10h do 6h.
- 5) Kurs – Sztuczna inteligencja – zmniejszenie liczby godzin wykładu na studiach stacjonarnych z 30h na 20h.

semestr VI

- 1) Kurs – Kryptografia – zmiana formy zaliczenia z egzaminu (E) na zaliczenie z oceną (zo); na studiach niestacjonarnych zwiększenie liczby godzin wykładu z 10h do 15h, zmniejszenie liczby godzin ćwiczeń laboratoryjnych z 15h do 10h
- 2) Kurs – Inżynieria i analiza danych – zmniejszenie liczby godzin laboratoryjnych z 45h na 30h (studia stacjonarne sem. VII) z 30h na 20h (studia niestacjonarne)
- 3) Kurs – Sztuczna inteligencja – zmniejszenie liczby godzin ćwiczeń laboratoryjnych na studiach niestacjonarnych z 30h na 20h.

semestr VII

- 1) Kurs – Praktyczne zastosowania sztucznej inteligencji – zmniejszenie liczby godzin laboratoryjnych na studiach stacjonarnych z 40h na 30h, na studiach niestacjonarnych z 30h na 20h

Kierunek CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW INŻYNIERSKICH 1-go stopnia 2023-2027

STUDIA STACJONARNE, STUDIA NIESTACJONARNE

semestr V

- 1) Kurs – Inżynieria oprogramowania – usunięcie z planu studiów.

- 2) Kurs – Kryptografia – zmiana liczby godzin ćwiczeń laboratoryjnych na studiach stacjonarnych z 15h do 20h, na studiach niestacjonarnych z 10h do 15h, punktów ECTS z 3 na 4; zmiana formy zaliczenia z zaliczenia z oceną (zo) na egzamin (E)
- 3) Kurs - Sprzętowe aspekty cyberbezpieczeństwa – zwiększenie liczby punktów ECTS z 2 na 3.

Kursy do wyboru

- 4) Kursy Programowanie aplikacji mobilnych oraz Tworzenie aplikacji internetowych – zmniejszenie liczby godzin wykładu z 20h na 5h (stacjonarne) oraz z 10h na 5h (niestacjonarne).

Kierunek CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW INŻYNIERSKICH 1-go stopnia 2024-2028

STUDIA STACJONARNE, STUDIA NIESTACJONARNE

semestr III

- 1) Zamiana kursów między semestrami – kurs - Programowanie niskopoziomowe przeniesiony z semestru 3 na semestr 4, kurs – Teoria informacji i kodowania z semestru 4 na semestr 3 (zmniejszenie liczby ECTS z 4 na 3 i zmiana formy zaliczenia z E na zo)

Kursy do wyboru

- 2) Technologie DevOps oraz Wprowadzenie do technologii chmury – zmniejszenie liczby godzin wykładu z 15h na 10h (stacjonarne) i z 10h na 6h (studia niestacjonarne)

semestr IV

- 1) Kurs Bezpieczeństwo systemów operacyjnych – zwiększenie liczby punktów ECTS z 2 na 3
- 2) Kurs - Fizyka i elektronika – zmiana liczby godzin:
 - wykładu – na studiach stacjonarnych z 30h na 20h, na studiach niestacjonarnych z 20h na 15h,
 - ćwiczeń laboratoryjnych – na studiach stacjonarnych z 30h na 35h, na studiach niestacjonarnych z 20h na 25h.

Semestr VII

- 1) Kurs – Militarny wymiar cyberbezpieczeństwa – zmiana formy zaliczenia z zaliczenia z oceną (zo) na zaliczenie (z), zmniejszenie liczby godzin punktów ECTS z 3 na 2.

Kursy do wyboru

- 2) Systemy i narzędzia autentyfikacji oraz Bezpieczeństwo handlu elektronicznego, bankowości i systemów płatności – zwiększenie liczby punktów ECTS z 2 na 3

Kierunek INFORMATYKA

PLAN STUDIÓW INŻYNIERSKICH 1-go stopnia 2024-2028

STUDIA STACJONARNE, STUDIA NIESTACJONARNE

Semestr V

- 1) Kurs – Wprowadzenie do technologii chmury (studia stacjonarne sem. V, studia niestacjonarne sem. VI) – zwiększenie liczby punktów ECTS z 5 na 6.
- 2) Kurs - Tworzenie aplikacji internetowych 2 - – zwiększenie liczby punktów ECTS z 4 na 5.

Semestr VII

- 1) Kurs – Współczesne narzędzia sztucznej inteligencji w przetwarzaniu danych (studia stacjonarne sem. VII, studia niestacjonarne sem. VI) – usunięcia kursu z planu studiów
- 2) Kurs – Praktyczne zastosowania sztucznej inteligencji ze specjalności Data Science (sem.VII) zostaje przeniesiony na plan główny na sem. VII w wymiarze godzinowym wykład 20h (stacjonarne) 10h (niestacjonarne) oraz ćwiczeń laboratoryjnych 30h (stacjonarne) 20h (niestacjonarne)
- 3) Kurs - Technologie decentralizacji danych (Blockchain) (studia stacjonarne sem. VII, studia niestacjonarne sem. VI) – zmniejszenie liczby punktów ECTS z 5 na 4.

Specjalność: Inżynieria oprogramowania

Semestr IV

- 1) Kurs – Analiza danych – zmiana formy ćwiczeń z audytoryjnych na laboratoryjne.

Semestr V

- 1) Kurs – Architektura oprogramowania – (studia stacjonarne sem. V, studia niestacjonarne sem. VI) - usunięcie kursu z planu studiów.
- 2) Jakość i testowanie oprogramowania (studia stacjonarne sem. V, studia niestacjonarne sem. VI) – zwiększenie liczby punktów ECTS z 3 na 4.

Semestr VII

- 3) Kurs – Tworzenie gier komputerowych – zwiększenie liczby punktów ECTS z 4 na 5; zmniejszenie liczby godzin ćwiczeń laboratoryjnych na studiach stacjonarnych z 40h na 30h

Specjalność: Data Science

Semestr V

- 2) Kurs – Analiza danych oparta na sztucznej inteligencji – przeniesienie na semestr VII, zwiększenie liczby punktów ECTS z 4 do 5.
- 3) Kurs - Metody zbierania informacji – zwiększenie liczby punktów ECTS z 2 do 4.
- 4) Kurs – Przetwarzanie języka naturalnego – zmniejszenie liczby wykładów z 15h na 10h (stacjonarne) i 10h na 6h (niestacjonarne) oraz zwiększenie liczby ćwiczeń laboratoryjnych z 15h na 20h (stacjonarne) i z 10h na 15h (niestacjonarne)

Korekty obowiązują od roku akademickiego 2025/2026.

