CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

PROGRAM STUDIÓW WYŻSZYCH ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM 2025/2026

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:

	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).

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

	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 C*yberbezpieczeństwo* 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 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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	10	10						20	zo	2
Teoria bezpieczeństwa	10	10						20	z	2
Ochrona własności intelektualnej							15	15	z	1
	80	**105**		**40**			**15**	**240**	**1**	**25**

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	3
Programowanie funkcyjne (Python)										
Wykład z zakresu nauk humanistycznych lub społecznych	10							10	z	2
	16			**20**				**36**		**5**

Pozostałe zajęcia

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

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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	4
Algorytmy i struktury danych	20			20				40	E	5
Organizacja i architektura komputerów	15			20				35	zo	4
Wprowadzenie do sieci komputerowych	6			20				26	zo	3
Programowanie obiektowe	15			20				35	E	4
Standaryzacja systemów cyberbezpieczeństwa		15						15	zo	2
Środowisko cyberbezpieczeństwa	15	10						25	z	3
	91	**55**		**80**				**226**	**3**	**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**

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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
Programowanie niskopoziomowe				20				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
	71	**50**		**80**				**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**

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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				
Teoria informacji i kodowania	10			10				20	E	4
Bezpieczeństwo systemów operacyjnych	10			10				20	zo	2
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
	61	**20**		**100**				**181**	**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 - 3			30					30	E	4
Manipulacja informacją		15						15	z	2
Kultura informacyjna w cyberbezpieczeństwie										
		15	**30**					**45**	**1**	**6**

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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 elektonicznych	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. **Termin: praktyka nieciągła w trakcie całego semestru**	240		z	10
	240			**10**

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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 cyberatakom	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**	**0**	**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**	**0**	**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		**0**	**10**

PLAN STUDIÓW NIESTACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2025-2029

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2025/2026

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**	**0**	**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**	**0**	**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

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. 27.02.2026 r.

Uchwała nr 3/IBiI/26
Rady Instytutu Bezpieczeństwa i Informatyki
Uniwersytetu Komisji Edukacji Narodowej w Krakowie
z dnia 27 stycznia 2026 r.

Rada Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie podjęła uchwałę w sprawie zatwierdzenia korekt w programach i planach studiów na kierunkach:

1. Informatyka 1 stopnia cyklu 2025-26 (studia stacjonarne i niestacjonarne) – korekty od 2 semestru studiów;
2. Cyberbezpieczeństwo 1 stopnia cyklu 2025-26 (studia stacjonarne i niestacjonarne) – korekty od 2 semestru studiów;
3. Informatyka 2 stopnia cyklu 2025-26 (studia stacjonarne i niestacjonarne) – korekty od 1 semestru studiów.

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

Uniwersytet Komisji Edukacji Narodowej w Krakowie

Instytut Bezpieczeństwa i Informatyki

ul. Podchorążych 2, 30-084 Kraków, tel. 12-662-78-45, e-mail: ii@uken.krakow.pl

Zał. do uchwały nr 3/IBiI/2026

Korekty w planach studiów
Kierunków: Informatyka I i II stopnia oraz Cyberbezpieczeństwo I stopnia
Studia stacjonarne i niestacjonarne
dla cykli: 2025-2026

Kierunek INFORMATYKA - PLAN STUDIÓW 2-go stopnia cykl 2025-2026

semestr 1

1. Kurs *Projektowanie inżynierskie w Informatyce* zmienia nazwę na *Projektowanie i inżynieria systemów informatycznych*.

Kierunek INFORMATYKA - PLAN STUDIÓW 1-go stopnia cykl 2025-2026

semestr 2

1. Kurs *Matematyka 1*
   - na studiach stacjonarnych - zwiększenie liczby godzin wykładu z 24h na 25h, zwiększenie liczby godzin ćwiczeń audytoryjnych z 36h na 40h;
   - zmniejszenie liczby punktów ECTS z 5 na 4.
2. Kurs *Podstawy programowania w języku Python*
   - na studiach stacjonarnych - zwiększenie liczby godzin wykładu z 10h na 15h;
   - zmniejszenie liczby punktów ECTS z 4 na 3.
3. Kurs *Grafika komputerowa*
   - na studiach stacjonarnych - zwiększenie liczby godzin ćwiczeń laboratoryjnych z 30h na 35h.
4. Kurs *Programowanie obiektowe*
   - zmniejszenie liczby punktów ECTS z 6 na 5.
5. Dodanie nowego kursu o nazwie - *Fizyka i elektronika II* w wymiarze:
   - na studiach stacjonarnych: 15h wykładów, 25h ćwiczeń laboratoryjnych, 3 punkty ECTS;
   - na studiach niestacjonarnych: 10h wykładów, 15h ćwiczeń laboratoryjnych, 3 punkty ECTS;
   - forma zaliczenia - zaliczenie z oceną.

semestr 3

1. Kurs *Matematyka 2*
   - na studiach stacjonarnych - zwiększenie liczby godzin wykładu z 25h na 30h, zwiększenie liczby godzin audytoryjnych z 30h na 35h.
2. Kurs *Organizacja baz danych i wiedzy*
   - zmniejszenie liczby godzin ECTS z 4 na 2.
3. Kurs *Wprowadzenie do sieci komputerowych*
   - zmniejszenie liczby godzin ECTS z 3 na 2.
4. Dodanie nowego kursu o nazwie - *Narzędzia praktyki inżynierskiej w wymiarze*:
   - na studiach stacjonarnych 25h ćwiczeń laboratoryjnych, 1 punkt ECTS;
   - na studiach niestacjonarnych 15h ćwiczeń laboratoryjnych, 1 punkt ECTS;
   - forma zaliczenia - zaliczenie z oceną.

Uniwersytet Komisji Edukacji Narodowej w Krakowie

Instytut Bezpieczeństwa i Informatyki

ul. Podchorążych 2, 30-084 Kraków, tel. 12-662-78-45, e-mail: ii@uken.krakow.pl

semestr 3 - specjalność Inżynieria oprogramowania

1. Kurs *Języki skryptowe*
   - zwiększenie liczby punktów ECTS z 2 na 3;
   - dodanie wykładu w wymiarze - na studiach stacjonarnych 15h, na studiach niestacjonarnych 10h.
2. Kurs Programowanie obiektowe w języki Python
   - zwiększenie liczby godzin wykładu - na studiach stacjonarnych z 20h na 30h, na studiach niestacjonarnych z 10h na 15h.

semestr 3 - specjalność Data Science

1. Kurs *Podstawy Data Science*
   - na studiach stacjonarnych - zwiększenie godzin wykładu z 20h na 25h;
   - na studiach niestacjonarnych - zwiększenie godzin wykładu z 10h na 15h.
2. Kurs *Wizualizacja danych*
   - zwiększenie liczby punktów ECTS z 2 na 3;
   - na studiach stacjonarnych - zwiększenie godzin wykładu z 10h na 15h, zwiększenie liczby godzin ćwiczeń laboratoryjnych z 20h na 25h;
   - na studiach niestacjonarnych - zwiększenie godzin wykładu z 6h na 10h.

semestr 4

1. Kurs *Podstawy sztucznej inteligencji*
   - zwiększenie liczby punktów ECTS z 3 na 4;
2. Kurs Administracja i integracja systemów operacyjnych
   - zmniejszenie liczby punktów ECTS z 3 na 2;
3. Dodanie nowego kursu o nazwie – *Projektowanie systemów wbudowanych* w wymiarze:
   - na studiach stacjonarnych: 10h wykładów, 30h ćwiczeń laboratoryjnych, 2 punkty ECTS;
   - na studiach niestacjonarnych: 6h wykładów, 15h ćwiczeń laboratoryjnych, 2 punkty ECTS;
   - forma zaliczenia - zaliczenie z oceną.

semestr 4 - specjalność Inżynieria oprogramowania

1. Kurs *Tworzenie aplikacji mobilnych*
   - dodanie wykładu w wymiarze - na studiach stacjonarnych 10h, na studiach niestacjonarnych 5h;
2. Kurs *Analiza danych*
   - zwiększenie liczby punktów ECTS z 3 na 4.
   - na studiach stacjonarnych zwiększenie liczby godzin wykładu z 15h na 20h;
   - zwiększenie liczby godzin ćwiczeń laboratoryjnych – na studiach stacjonarnych z 15 na 25, na studiach niestacjonarnych z 10h na 15h.
3. Dodanie nowego kursu o nazwie *Optymalizacja modeli uczenie maszynowego* w wymiarze:
   - 4 punkty ECTS;
   - na studiach niestacjonarnych 20h ćwiczeń laboratoryjnych;
   - na studiach stacjonarnych kurs będzie realizowany w semestrze V
   - forma zaliczenia - egzamin
4. Usunięcie z planu studiów kursu *Programowanie systemowe*.

Uniwersytet Komisji Edukacji Narodowej w Krakowie

Instytut Bezpieczeństwa i Informatyki

ul. Podchorążych 2, 30-084 Kraków, tel. 12-662-78-45, e-mail: ii@uken.krakow.pl

semestr 4 - specjalność Data Science

1. Kurs *Analiza systemowa i modelowanie systemów*
   - zmniejszenie liczby punktów ECTS z 4 na 3;
   - zmiana formy zaliczenia z egzaminu na zaliczenie z oceną;
   - na studiach stacjonarnych - zwiększenie liczby godzin wykładu z 10h 15h, zwiększenie liczby godzin ćwiczeń laboratoryjnych z 20h na 25h;
   - na studiach niestacjonarnych - zwiększenie liczby godzin wykładu z 6h 10h.
2. Kurs *Analiza danych z językiem SQL*
   - zwiększenie liczby punktów ECTS z 3 na 4;
   - dodanie wykładu w wymiarze – na studiach stacjonarnych 10h, na studiach niestacjonarnych 5h
   - zwiększenie liczby godzin ćwiczeń laboratoryjnych – na studiach stacjonarnych z 30h na 40h, na studiach niestacjonarnych z 20h na 25h.
3. Dodanie kursu Optymalizacja modeli uczenia maszynowego w DS. w wymiarze:
   - 4 punkty ECTS;
   - Forma zaliczenia – egzamin;
   - na studiach niestacjonarnych – 20h ćwiczeń laboratoryjnych;
   - na studiach stacjonarnych kurs będzie realizowany w semestrze V.
4. Usunięcie kursu *Internet Rzeczy*

semestr 5

1. Kurs *Wprowadzenie do technologii chmury*
   - Zmniejszenie liczby punktów ECTS z 6 na 4;
   - na studiach stacjonarnych: zwiększenie liczby godzin wykładu z 10h do 20h;
   - na studiach niestacjonarnych: przeniesienie kursu z semestru VI na semestr V, zwiększenie liczby godzin wykładu z 6h na 10h.
2. Kurs *Tworzenie aplikacji internetowych 2*
   - zmniejszenie liczby punktów ECTS z 5 na 2.
3. Dodanie nowego kursu o nazwie - *Metody statystyczne w Informatyce* w wymiarze:
   - 3 punkty ECTS;
   - na studiach stacjonarnych: 20h wykładów, 30h ćwiczeń laboratoryjnych;
   - na studiach niestacjonarnych – kurs będzie realizowany w semestrze VI.

semestr 5 - specjalność Inżynieria oprogramowania

1. Kurs *Programowanie sieciowe*
   - zmniejszenie liczby punktów ECTS z 4 na 3
   - dodanie wykładu – na studiach stacjonarnych w wymiarze 10h, na studiach niestacjonarnych w wymiarze 5h.
2. Dodanie nowego kursu o nazwie *Optymalizacja modeli uczenie maszynowego w IO* w wymiarze:
   - 4 punkty ECTS;
   - na studiach stacjonarnych 30h ćwiczeń laboratoryjnych;
   - na studiach niestacjonarnych kurs realizowany w semestrze IV;
   - forma zaliczenia - egzamin
3. Kurs *Jakość i testowanie oprogramowania*
   - zmniejszenie liczby punktów ECTS z 4 na 3;
   - dodanie wykładu w wymiarze – na studiach stacjonarnych 10h, na studiach niestacjonarnych 5h;
   - na studiach stacjonarnych zwiększenie liczby godzin ćwiczeń laboratoryjnych z 25h na 30h

Uniwersytet Komisji Edukacji Narodowej w Krakowie

Instytut Bezpieczeństwa i Informatyki

ul. Podchorążych 2, 30-084 Kraków, tel. 12-662-78-45, e-mail: ii@uken.krakow.pl

semestr 5 - specjalność Data Science

1. Kurs Metody zbierania informacji
   - zmniejszenie liczby punktów ECTS z 4 na 3;
   - zwiększenie liczby godzin wykładu – na studiach stacjonarnych z 10h na 20h, na studiach niestacjonarnych z 6h na 10h.
2. Kurs Przetwarzanie języka naturalnego
   - zmniejszenie liczby punktów ECTS z 4 na 3
   - na studiach stacjonarnych - zwiększenie liczby godzin zajęć laboratoryjnych z 20h na 30h;
3. Dodanie nowego kursu o nazwie – *Optymalizacja modeli uczenia maszynowego w DS.*
   - 4 punkty ECTS;
   - na studiach stacjonarnych 30h ćwiczeń laboratoryjnych;
   - forma zaliczenia – egzamin;
   - na studiach niestacjonarnych – kurs będzie realizowany w semestrze IV.

semestr 6

1. Dodanie nowego kursu o nazwie - *Metody statystyczne w Informatyce w wymiarze:*
   - 3 punkty ECTS;
   - na studiach niestacjonarnych: 10h wykładów, 15h ćwiczeń laboratoryjnych.
2. Dodanie nowego kursu o nazwie - *Wzorce projektowe* w wymiarze:
   - 1 punkt ECTS;
   - na studiach niestacjonarnych – 15h godzin ćwiczeń laboratoryjnych;
   - na studiach stacjonarnych – kurs będzie realizowany w semestrze VII.
3. Kurs *Technologie decentralizacji danych (Blockchain)*
   - na studiach niestacjonarnych - zwiększenie liczby godzin ćwiczeń laboratoryjnych z 15h na 20h;
   - na studiach na studiach stacjonarnych – kurs jest realizowany w semestrze VII.

semestr 6 - specjalność Inżynieria oprogramowania

1. Kurs *Tworzenie gier komputerowych*
   - na studiach niestacjonarnych – przeniesienie z semestru VII na semestr VI;
   - na studiach niestacjonarnych - zwiększenie liczby godzin wykładu z 10h na 15h.

semestr 7

1. Dodanie nowego kursu o nazwie - *Wzorce projektowe* w wymiarze:
   - 1 punkt ECTS;
   - na studiach stacjonarnych w wymiarze 20h;
   - na studiach niestacjonarnych – kurs jest realizowany w semestrze VI.
2. Kurs *Technologie DevOps*
   - na studiach stacjonarnych zwiększenie liczby godzin wykładu z 10h na 20h;
   - na studiach niestacjonarnych zwiększenie liczby godzin wykładu z 6h na 10h.
3. Kurs *Technologie decentralizacji danych (Blockchain)*
   - na studiach stacjonarnych zwiększenie liczby godzin ćwiczeń laboratoryjnych z 25h na 30h

semestr 6 - specjalność Data Science

1. Kurs Przetwarzanie języka naturalnego
   - zmniejszenie liczby punktów ECTS z 4 na 3
   - na studiach niestacjonarnych – zmniejszenie liczby godzin wykładu z 6h na 5h, zwiększenie liczby godzin zajęć laboratoryjnych z 15h na 20h.

2. Kurs *Analiza danych oparta na sztucznej inteligencji*
    - na studiach niestacjonarnych przeniesienie kursu z semestru VII na VI
    - na studiach niestacjonarnych – zwiększenie liczby godzin wykładu z 10h na 15h, zwiększenie liczby godzin ćwiczeń laboratoryjnych z 20h na 25h.

semestr 7 - specjalność Inżynieria oprogramowania

1. Kurs *Tworzenie gier komputerowych*
    - na studiach stacjonarnych - zwiększenie liczby godzin wykładu z 20h na 25h.
2. Kurs *Projekt inżynierski*
    - na studiach stacjonarnych zwiększenie liczby godzin ćwiczeń seminaryjnych z 45h na 60h;
    - na studiach niestacjonarnych zwiększenie liczby godzin ćwiczeń seminaryjnych z 30h na 60h

semestr 7 - specjalność Data Science

1. Kurs *Analiza danych oparta na sztucznej inteligencji*
    - Na studiach stacjonarnych – zwiększenie liczby godzin ćwiczeń laboratoryjnych z 25h na 40h;
2. Kurs *Projekt inżynierski*
    - na studiach stacjonarnych zwiększenie liczby godzin ćwiczeń seminaryjnych z 45h na 60h;
    - na studiach niestacjonarnych zwiększenie liczby godzin ćwiczeń seminaryjnych z 30h na 60h.

Kierunek CYBERBEZPIECZEŃSTWO - PLAN STUDIÓW 1-go stopnia cykl 2025-2026

semestr 2

1. Kurs *Matematyka 1*
    - na studiach stacjonarnych - zwiększenie liczby godzin wykładu z 24h na 25h, zwiększenie liczby godzin ćwiczeń audytoryjnych z 36h na 40h
    - zmniejszenie liczby punktów ECTS z 5 na 4
2. Kurs *Środowisko cyberbezpieczeństwa*
    - zwiększenie liczby punktów ECTS z 2 na 3Korekty obowiązują od 1 semestru roku akademickiego 2025/2026.

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

Kraków 26.01.2026 r.

OPINIA nr .3../RJK/..26

Rady Jakości Kształcenia dla kierunku

INFORMATYKA i CYBERBEZPIECZEŃSTWO

dotyczy

planów i programów studiów

kierunków Informatyka i Cyberbezpieczeństwo

studia I i II stopnia stacjonarne i niestacjonarne

Instytutowa Rada Jakości Kształcenia pozytywnie opiniuje korekty w planach studiów:

1. Informatyka 2 stopnia (stacjonarne i niestacjonarne) nabór 2025-26 - korekty od 1 semestru
2. Informatyka 1 stopnia (stacjonarne i niestacjonarne) nabór 2025-26 - korekty od 2 semestru
3. Cyberbezpieczeństwo 1 stopnia (stacjonarne i niestacjonarne) nabór 2025-26 - korekty od 2 semestru.

Szczegółowe wyniki głosowania nad akceptacją programów i planów:

Liczba uprawnionych do głosowania: 13
Liczba oddanych głosów: 12
Akceptuję: 12
Nie akceptuję: 0
Wstrzymuję się: 0

Z-CA DYREKTORA
Instytutu Bezpieczeństwa i Informatyki
Krzaczek Beata
dr Beata Krzaczek

samorząd
studentów

Uniwersytetu Komisji
Edukacji Narodowej
w Krakowie

Kraków, 28.01.2026

Opinia Instytutowej Rady Samorządu Studentów nr 2/IRSS/26
Instytutu Bezpieczeństwa i Informatyki
Uniwersytetu Komisji Edukacji Narodowej w Krakowie

w sprawie korekty w planach studiów od semestru 2 dla kierunku Cyberbezpieczeństwo 1 stopnia cyklu 2025-26 (studia stacjonarne i niestacjonarne).

Na podstawie dostarczonych źródeł Instytutowa Rada Samorządu Studentów Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie dokonała oceny korekt w planach studiów od semestru 2 dla kierunku Cyberbezpieczeństwo 1 stopnia cyklu 2025-26 (studia stacjonarne i niestacjonarne) i wyraża pozytywną opinię na ich temat.

Dawid Chawrona

Członek Instytutowej Rady Samorządu Studentów
Instytutu Bezpieczeństwa i Informatyki

Podpis:

Dawid Chawrona

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

Uniwersytet Komisji Edukacji Narodowej w Krakowie

Uchwała nr 5.23.02.2026
Senatu
Uniwersytetu Komisji Edukacji Narodowej w Krakowie
z dnia 23 lutego 2026 roku

w sprawie: korekty harmonogramu realizacji programu kierunku studiów pierwszego stopnia Cyberbezpieczeństwo, profil praktyczny, edycja 2025/2026

Działając na podstawie art. 28 ust. 1 punkt 11 Ustawy z dnia 20 lipca 2018 roku – Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 poz. 1571), § 7 ust. 1. Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz. U. z 2023 poz. 2787) oraz § 23 pkt 23 Statutu Uczelni, po uzyskaniu opinii samorządu studenckiego i instytutowej rady ds. jakości kształcenia, Senat Uniwersytetu Komisji Edukacji Narodowej w Krakowie postanawia, co następuje:

§ 1

Senat dokonuje korekty harmonogramu realizacji programu kierunku studiów: Cyberbezpieczeństwo studia pierwszego stopnia, profil praktyczny, edycja 2025/2026. Zmiany wykazane w załączniku nr 1 do niniejszej uchwały.

§ 2

Skorygowany harmonogram realizacji programu kierunku studiów, o którym mowa w § 1, stanowi załączniki nr 2 i 3 do niniejszej uchwały.

§ 3

Uchwała wchodzi w życie od roku akademickiego 2025/2026 (semestr II).

p.o. Rektor
W. Bąk
dr hab. Wojciech Bąk, prof. UKEN

Korekta dotyczy:

semestr 2

1. Kurs *Matematyka 1*
- na studiach stacjonarnych: zwiększenie liczby godzin wykładu z 24h na 25h, zwiększenie liczby godzin ćwiczeń audytoryjnych z 36h na 40h,
    - na studiach stacjonarnych i niestacjonarnych: zmniejszenie liczby punktów ECTS z 5 na 4.
2. Kurs *Środowisko cyberbezpieczeństwa*
    - na studiach stacjonarnych i niestacjonarnych: zwiększenie liczby punktów ECTS z 2 na 3.