CYBERBEZPIECZEŃSTWO – studia niestacjonarne I stopnia

PROGRAM STUDIÓW WYŻSZYCH ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM 2023/2024

data zatwierdzenia przez Radę Instytutu

pieczęć i podpis Dyrektora

……

Studia wyższe na kierunku	Cyberbezpieczeństwo
Dziedzina/y	Nauk ścisłych i przyrodniczych, nauk inżynieryjno-technicznych, nauk społecznych
Dyscyplina wiodąca (% udział)	Informatyka techniczna i telekomunikacja (55%)
Pozostałe dyscypliny (% udział)	Nauki o bezpieczeństwie (30%), Informatyka (10%), Matematyka (5%),
Poziom	PIERWSZY (studia inżynierskie I stopnia)
Profil	praktyczny
Forma prowadzenia	STUDIA niestacjonarne
Specjalności	–
Punkty ECTS	210
Czas realizacji (liczba semestrów)	7
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 lub informatyki – 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: Mierny- 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 Pedagogicznego 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 i urządzeń sieciowych w lokalnych i rozległych sieciach komputerowych	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	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).

	również przykłady je ilustrujące oraz zależności występujące w obrębie wiedzy dotyczącej bezpieczeństwa w cyberprzestrzeni		
K_W08	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_W09	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_W10	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	indywidualnie lub w zespole pracować (m.in. opracować dokumentację, przedstawić prezentację i prowadzić dyskusję na temat zadania, projektu lub zagadnień w szczególności zw. z cyberbezpieczeństwem, również w jęz. obcym) lub 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 cyberbeczpieczeństwem	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 bezpieczeństwem w cyberprzestrzeni, 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 technologii w ujęciu historycznym, politycznym, społecznym, gospodarczym, militarnym, prawnym (w tym w zakresie ochrony własności intelektualnej) i etycznym	P6U_U	P6S_UW
K_U12	posługiwać się co najmniej jednym językiem obcym na poziomie	P6U_U	P6S_UK

	B2 Europejskiego Systemu Opisu Kształcenia Językowego oraz terminologią w zakresie cyberbezpieczeństwa		
K_U13	samodzielnie planować i realizować własne uczenie się oraz swój dalszy 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

Sylwetka absolwenta	Absolwent kierunku *cyberbezpieczeństwo* 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: • kryptografii, • tworzenia, konfiguracji i wykorzystania narzędzi oraz technologii związanych z bezpieczeństwem systemów oraz sieci komputerowych lokalnych i rozległych (w celu zabezpieczania ich funkcjonowania w instytucjach publicznych oraz u wszelkiego rodzaju podmiotów prowadzących działalność gospodarczą), • działania aplikacji i usług elektronicznych w Internecie (a także w sieciach o mniejszym zasięgu, w tym lokalnych), • dostępnych rozwiązań w obszarze zabezpieczeń sieci teleinformatycznych, systemów komputerowych, aplikacji oraz projektowania tego typu systemów. 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 technologii informacyjno-komunikacyjnych w ramach sieci teleinformatycznych, systemów operacyjnych i 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 teleinformatycznych przed atakami oraz

	dokonywania analizy struktur wrażliwych, w tym sieci komputerowych, w kontekście ich podatności na ataki, • 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, • w policyjnych wydziałach do walki z cyberprzestępczością, 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 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 *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 2023-2027

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2023/2024

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				
Matematyka 1		20						20	zo	3
Organizacja i architektura komputerów	15			20				35	E	4
Podstawy programowania	15			20				35	E	4
Teoretyczne podstawy informatyki	15	25						40	E	6
Teoria bezpieczeństwa	10	10						20	z	2
Ochrona własności intelektualnej							15	15	z	1
Technologie informacyjne				20				20	zo	3
	55	**55**		**60**			**15**	**185**	**3**	**23**

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Języki hipertekstowe i tworzenie stron WWW	10			20				30	zo	2
Systemy CMS										
Przedmioty z zakresu nauk humanistycznych	20	20						40	zo	5
	30	**20**		**20**				**70**		**7**

Pozostałe zajęcia

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

CYBERBEZPIECZEŃSTWO

6		

CYBERBEZPIECZEŃSTWO

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 2	20	30						50	E	5
Algorytmy i struktury danych	15			25				40	zo	6
Wprowadzenie do sieci komputerowych	10			10				20	zo	3
Bazy danych 1	10			20				30	zo	2
Języki i narzędzia programowania obiektowego	10			20				30	zo	2
Środowisko cyberbezpieczeństwa	20	10						30	E	4
Teoria organizacji i zarządzania	10	10						20	z	2
	95	**50**		**75**				**220**	**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				
Zarządzanie bezpieczeństwem informacji	5	10						15	z	3
Zarządzanie ryzykiem cyberbezpieczeństwa										
Język obcy B2 -1			30					30	z	3
	5	**10**	**30**					**45**		**6**

CYBERBEZPIECZEŃSTWO

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 3	15	30						45	zo	5
Wprowadzenie do systemów operacyjnych	15			20				35	zo	4
Bezpieczeństwo aplikacji internetowych 1	15			20				35	E	3
Bezpieczeństwo sieci komputerowych 1	10			20				30	E	3
Bezpieczeństwo systemów operacyjnych 1	15			20				35	zo	3
Nowe technologie w cyberprzestrzeni	15	10						25	z	3
Ochrona danych osobowych	10	10						20	z	3
	95	**50**		**80**				**225**	**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
Patologie w cyberprzestrzeni	10	10						20	z	3
Cyberzagrożenia										
	10	**10**	**30**					**50**		**6**

CYBERBEZPIECZEŃSTWO

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				
Bazy danych 2				20				20	zo	3
Bezpieczeństwo aplikacji internetowych 2				20				20	zo	2
Bezpieczeństwo sieci komputerowych 2				20				20	zo	3
Programowanie niskopoziomowe	10			10				20	zo	3
Programowanie skryptowe	10			20				30	zo	4
Teoria informacji i kodowania	10			15				25	zo	3
Zarządzanie kryzysowe w cyberbezpieczeństwie	10	15						25	E	4
Biały wywiad		15						15	z	2
	40	**30**		**105**				**175**	**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

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				
Kryptografia	15			10				30	zo	3
Inżynieria oprogramowania	10			15				25	zo	2
Podstawy prawne cyberbezpieczeństwa	15	10						25	E	4
Zarządzanie strategiczne w cyberbezpieczeństwie	10	15						25	E	4
	50	**25**		**25**				**105**	**2**	**13**

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Komunikacja i zarządzanie projektami / *Metody badawcze w informatyce i projektach inżynierskich*	10	10						20	zo	3
Programowanie aplikacji mobilnych / *Tworzenie aplikacji internetowych*	10			20				30	zo	4
	20	**10**		**20**				**50**		**7**

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. Zasady odbywania praktyk normuje Regulamin praktyk zawodowych (niepedagogicznych) Studentów Uniwersytetu Pedagogicznego im. KEN oraz Regulamin Studenckich Praktyk Zawodowych. **Praktyka nieciągła w trakcie całego semestru.**	240		z	10
	240			**10**

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 infrastruktury krytycznej i systemów sterowania przemysłowego i IoT	5			20				25	zo	3
Sprzętowe aspekty cyberbezpieczeństwa	5			15				20	zo	2
Bezpieczeństwo sieci komputerowych 3				20				20	zo	3
Bezpieczeństwo systemów operacyjnych 2				20				20	zo	3
Metodyki testów penetracyjnych				20				20	zo	2
Wykrywanie incydentów				10				10	zo	2
Militarny wymiar cyberbezpieczeństwa	15	10						25	E	4
	25			**105**				**140**	**1**	**19**

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. Zasady odbywania praktyk normuje Regulamin praktyk zawodowych (niepedagogicznych) Studentów Uniwersytetu Pedagogicznego im. KEN oraz Regulamin Studenckich Praktyk Zawodowych. **Praktyka nieciągła w trakcie całego semestru.**	240		z	10
	240			**10**

CYBERBEZPIECZEŃSTWO

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				
Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego	10			15				25	zo	3
Analiza malware	10			10				20	zo	3
Wojny informacyjne	10	10						20	z	2
	30	**10**		**25**				**65**		**8**

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Analiza informacji	10			20				30	zo	3
Metody eksploracji danych										
*Projekt inżynierski**					30			40	zo	5
	10			**20**	**30**			**70**		**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. Zasady odbywania praktyk normuje Regulamin praktyk zawodowych (niepedagogicznych) Studentów Uniwersytetu Pedagogicznego im. KEN oraz Regulamin Studenckich Praktyk Zawodowych. **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.	5

*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.inob.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. 21.06.2024 r.

Uchwała nr 9/IBiI/24
Rady Instytutu Bezpieczeństwa i Informatyki
Uniwersytetu Komisji Edukacji Narodowej w Krakowie
z dnia 21 czerwca 2024 r.

Rada Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie podjęła uchwałę w sprawie zatwierdzenia korekt w planach i programach studiów 1-go i 2-go stopnia na kierunku Informatyka oraz 1-go stopnia kierunku Cyberbezpieczeństwo. Korekty będą obowiązywały od roku akademickiego 2024/2025.

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 18.06.2024 r.

OPINIA

Rady ds. Jakości Kształcenia dla kierunków

INFORMATYKA i CYBERBEZPIECZEŃSTWO

dotyczy

planów i programów studiów

kierunku Informatyka oraz kierunku Cyberbezpieczeństwo

studia I i II stopnia stacjonarne i niestacjonarne

Instytutowa Rada ds. Jakości Kształcenia po zapoznaniu się z dokumentami pozytywnie opiniuje korekty w planach studiów 1 i 2 stopnia stacjonarnych i niestacjonarnych. Korekty w planach obowiązywać będą od roku akademickiego 2024-2025.

Skład Rady:

1. dr Beata Krzaczek (Przewodnicząca)
2. dr inż. Magdalena Andrzejewska (Koordynator ds. kierunku Informatyka)
3. dr hab. Serhii Semenov, prof. UKEN (Koordynator ds. kierunku Cyberbezpieczeństwo)

Z-CA DYREKTORA
Instytutu Bezpieczeństwa i Informatyki
dr Beata Krzaczek

Kraków, 20.06.2024 r.

OPINIA

Instytutowa Rada Samorządu Studenckiego Instytutu Bezpieczeństwa i Informatyki pozytywnie opiniuje korekty wprowadzone do planów studiów (rozpoczynających się od roku akademickiego 2021, 2022, 2023)od roku akademickiego 2024/2025 dla kierunków Informatyka 1 i 2 stopnia oraz kierunku Cyberbezpieczeństwo 1 stopnia.

Dawid Chawrona