

CYBERBEZPIECZEŃSTWO – studia stacjonarne 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 stacjonarne
Specjalności	–
Punkty ECTS	210
Czas realizacji (liczba semestrów)	7 semestrów
Uzyskiwany tytuł zawodowy	inżynier
Warunki przyjęcia na studia	<p>Kryteria przyjęć na studia dla kandydatów z „nową maturą”:</p> <p>Dla nowej matury: 1% = 1 punkt. O miejscu na liście rankingowej decyduje większa z liczb:</p> <ul style="list-style-type: none">wynik (w punktach) egzaminu maturalnego z matematyki – poziom podstawowy, część pisemna2 x wynik (w punktach) egzaminu maturalnego z matematyki lub informatyki – poziom rozszerzony, część pisemna. <p>Kryteria przyjęć na studia dla kandydatów ze „starą maturą”:</p> <p>o miejscu na liście rankingowej decyduje większa z liczb:</p> <ul style="list-style-type: none">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. <p>Przelicznik ocen ze świadectw starej matury na punkty:</p>

CYBERBEZPIECZEŃSTWO – studia stacjonarne I stopnia

	<p>Dopuszczający - 30 punktów Dostateczny - 50 punktów Dobry - 70 punktów Bardzo dobry - 90 punktów Celujący - 100 punktów</p> <p>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.</p>
--	--

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 stacjonarne 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 stacjonarne 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 dokończenia 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 stacjonarne I stopnia

<p>Sylwetka absolwenta</p>	<p>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:</p> <ul style="list-style-type: none"> • 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). <p>Ponadto zna zagrożenia cyberprzestrzeni i świata wirtualnego, w tym m.in.:</p> <ul style="list-style-type: none"> • aspekty prawne, kryminologiczne i techniczne cyberprzestępczości • patologiczne formy korzystania z mediów i cyberprzemocy • zagrożenia bezpieczeństwa informacyjnego. <p>Absolwent kierunku cyberbezpieczeństwo posiada umiejętności i kompetencje w zakresie:</p> <ul style="list-style-type: none"> • 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.
<p>Uzyskiwane kwalifikacje oraz uprawnienia zawodowe</p>	<p>Absolwenci tego kierunku studiów mogą podjąć pracę w obszarach związanych z bezpieczeństwem w cyberprzestrzeni (sektor prywatny/publiczny), w tym:</p> <ul style="list-style-type: none"> • 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.
<p>Dostęp do dalszych studiów</p>	<p>Absolwenci studiów I stopnia uzyskują przygotowanie do pracy zawodowej, a także możliwość kontynuowania kształcenia na studiach II stopnia na kierunku <i>Cyberbezpieczeństwo</i>, jak również pokrewnych kierunkach studiów oraz na studiach podyplomowych.</p>
<p>Jednostka badawczo-dydaktyczna właściwa merytorycznie dla tych studiów</p>	<p>Instytut Bezpieczeństwa i Informatyki</p>