

**PROGRAM SPECJALNOŚCI
STUDIÓW WYŻSZYCH
ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM
2024/2025**

| | |
|-----------------------------------------------------|--|
| zatwierdzony przez Radę Instytutu dnia | |
|-----------------------------------------------------|--|

| | |
|---------------------|---------------------------------------------------------|
| Nazwa specjalności | CYBERBEZPIECZEŃSTWO (CB) |
| Liczba punktów ECTS | 44 studia stacjonarne / 44 studia niestacjonarne |

Uzyskiwane kwalifikacje oraz uprawnienia zawodowe

| |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Absolwent kierunku informatyka, studia II stopnia po specjalności Cyberbezpieczeństwo 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.</p> <p>Absolwent posiada szerokie kompetencje nie tylko w dziedzinie informatyki i telekomunikacji (m.in. w zakresie bezpieczeństwa aplikacji internetowych, systemów komputerowych, aplikacji mobilnych oraz przemysłowych systemów transmisji danych, bezpieczeństwa chmur obliczeniowych oraz przetwarzania i ochrony danych typu Big Data), czy też aspektach prawnych i organizacyjnych (m.in. w zakresie zarządzania strategicznego firmą, w kontekście zagrożeń cyberbezpieczeństwa i wymogów ochrony danych), ale także w zakresie podnoszenia poziomu świadomości występowania cyberzagrożeń i możliwości zapobiegania ich gospodarczym, społecznym, psychologicznym i politycznym konsekwencjom.</p> <p>Absolwenci specjalności posiadają solidne podstawy wiedzy z zakresu szerokiego spektrum rozwiązań technologicznych security IT, niezbędnej do definiowania zagrożeń w cyberprzestrzeni i stosowania środków zapobiegawczych. Umieją diagnozować i analizować zagrożenia związane z bezpieczeństwem cyberprzestrzeni, a także stosować narzędzia służące do ich ograniczania i eliminacji. Poznali zasady polityki cyberbezpieczeństwa i sposoby jej kształtowania oraz zdobyli wiedzę dotyczącą mechanizmów, technologii i systemów zabezpieczeń przed cyberzagrozeniami.</p> <p>Studia na tej specjalności przygotowują pracowników dla sektora państwowego i prywatnego w kraju i za granicą realizującego zadania w obszarze cyberbezpieczeństwa oraz gospodarczego każdej branży mającej styczność z cyberprzestrzenią.</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,• w policyjnych wydziałach do walki z cyberprzestępczością,• eksperci działów IT ds. bezpieczeństwa m.in. jako:<ul style="list-style-type: none">✓ administratorzy sieci komputerowych,✓ specjaliści ds. bezpieczeństwa,✓ analitycy i konsultanci ds. cyberbezpieczeństwa,✓ inżynierowie bezpieczeństwa,✓ pentesterzy,✓ Security Software Developerzy – programiści z wiedzą nt. cyberbezpieczeństwa. <p>Absolwent jest przygotowany do podejmowania wyzwań badawczych i kontynuacji edukacji w szkole doktorskiej lub na studiach podyplomowych.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Efekty uczenia się dla specjalności

| WIEDZA Absolwent: | |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SC_W01 | ma wiedzę na temat zasad działania podstawowych narzędzi kryptograficznych i steganograficznych w kontekście zapewnienia zabezpieczenia struktur lokalnych i sieciowych. |
| SC_W02 | zna elementarne algorytmy, języki i techniki programowania oraz zasady projektowania systemów baz danych w kontekście wymagań bezpieczeństwa. |
| SC_W03 | zna zagadnienia dotyczące systemów informatycznych i sieci komputerowych oraz zasady ich organizacji i administracji ze szczególnym uwzględnieniem bezpieczeństwa systemów serwerowych i rozwiązań chmurowych. |
| SC_W04 | ma wiedzę na temat nowoczesnych technologii analizy, wykrywania i oceny ewentualnych zagrożeń oraz czynników destabilizujących przestrzeń i zasoby informacyjne zgodnie z ustaloną polityką bezpieczeństwa informacyjnego i/lub cyberbezpieczeństwa. |
| SC_W05 | ma pogłębioną wiedzę na temat znaczenia sztucznej inteligencji w ograniczaniu ryzyka występowania cyberzagrożeń i ich zapobieganiu. |
| SC_W06 | ma poszerzoną i pogłębioną wiedzę pozwalającą na zrozumienie konieczności przygotowania człowieka do świadomego, racjonalnego, bezpiecznego i etycznego funkcjonowania w społeczeństwie informacyjnym i cywilizacji cyfrowej (m.in. w zakresie aspektów działalności człowieka w cyberprzestrzeni w świetle prawa międzynarodowego). |
| SC_W07 | ma aktualną wiedzę na temat kluczowych zagadnień podlegających regulacji w przestrzeni cyfrowej oraz znaczenia nauk społecznych i czynnika ludzkiego w cyberbezpieczeństwie (w tym mechanizmów rządzących ludzkim umysłem i zachowaniem w kontekście nowych technologii). |
| UMIEJĘTNOŚCI Absolwent: | |
| SC_U01 | bada, opracowuje, wdraża i stosuje metody i środki kryptograficzne i steganograficzne ochrony informacji. |
| SC_U02 | potrafi konstruować algorytmy i pisać pojedyncze aplikacje oraz większe projekty programistyczne, w oparciu o języki programowania niskiego i wysokiego poziomu z uwzględnieniem zasad bezpieczeństwa. |
| SC_U03 | potrafi analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania. |
| SC_U04 | potrafi konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych. |
| SC_U05 | potrafi posługiwać się narzędziami do monitorowania procesów w systemach informatycznych i telekomunikacyjnych. |
| SC_U06 | opracowuje i wdraża projekty ochrony informacji w cyberprzestrzeni z wykorzystaniem sztucznej inteligencji. |
| SC_U07 | Potrafi myśleć krytycznie i argumentować swoje stanowisko. Identyfikuje regulacje prawne |

| | |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | cyberprzestrzeni z perspektywy międzynarodowej, wnikliwie analizuje normy prawne dotyczące cyberprzestrzeni ustanowione przez powszechne i regionalne organizacje międzynarodowe, w tym międzynarodowe organy ścigania oraz inne instytucje zainteresowane regulacją statusu przestrzeni wirtualnej. |
| SC_U8 | Potrafi dostrzec i scharakteryzować zagrożenia dla bezpieczeństwa informacyjnego związane z niskim poziomem kultury informacyjnej człowieka (m.in. opracować i zastosować schemat badania poziomu kultury informacyjnej) oraz postrzegania bezpieczeństwa w cyberprzestrzeni i psychologicznych konsekwencji tego procesu. |
| KOMPETENCJE SPOŁECZNE Absolwent: | |
| SC_K01 | ma świadomość roli społecznej absolwenta kierunku inżynierijno-technicznego. |
| SC_K02 | potrafi formułować opinie na temat zagadnień związanych z branżą informatyczną ze szczególnym uwzględnieniem aspektów cyberbezpieczeństwa. |
| SC_K03 | ma świadomość wagi profesjonalnego zachowania i przestrzegania zasad etyki zawodowej, prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu. |

| | |
|------------------------------------------------------------------------|----------------------------------------------|
| Jednostka badawczo-dydaktyczna właściwa merytorycznie dla tych studiów | INSTYTUT BEZPIECZEŃSTWA I INFORMATYKI |
|------------------------------------------------------------------------|----------------------------------------------|