KARTA ZGŁOSZENIA STUDIÓW PODYPLOMOWYCH

WYDZIAŁ: NAUK INŻYNIERYJNO-TECHNICZNYCH

INSTYTUT: STEROWANIA I SYSTEMÓW INFORMATYCZNYCH

NAZWA STUDIÓW PODYPLOMOWYCH: CYBERBEZPIECZEŃSTWO
STUDIA PODYPLOMOWE*: (zaznacz X)*
dodatkowa specjalność ☐ doskonalące ☒

PODGRUPA KIERUNKU STUDIÓW (wg załącznika) 061 podgrupa technologii teleinformacyjnych

KOD ISCED KIERUNKU (wg załącznika)
0612 Projektowanie i administrowanie baz danych i sieci
0613 Tworzenie i analiza oprogramowania i aplikacji
0619 Technologie teleinformacyjne gdzie indziej niesklasyfikowane
0714 Elektronika i automatyka

CZAS TRWANIA: 2 SEMESTRY
OPŁATA ZA SEMESTR: 5450,00zł
OPŁATA REKRUTACYJNA: 85,00zł

REKRUTACJA: Kandydaci na studia zobowiązani są do elektronicznej rejestracji a następnie złożenia wymaganych dokumentów w Sekretariacie Wydziału Nauk Inżynieryjno-Technicznych (ul. Z. Szafrana 2, budynek A-2, pokój 12). Rekrutacja odbywa się na podstawie kolejności zgłoszeń. Warunkiem uruchomienia studiów jest uzyskanie deklaracji uczestnictwa przez odpowiednią liczbę słuchaczy.
LIMIT MIEJSC: min: 15 max: 30.
WYMAGANE DOKUMENTY: 1) podanie o przyjęcie na studia, 2) odpis dyplomu ukończenia studiów wyższych: I stopnia lub II stopnia lub jednolitych magisterskich, 3) dowód wpłaty opłaty rekrutacyjnej, 4) zobowiązanie do ponoszenia kosztów odpłatności za studia.

TERMIN SKŁADANIA DOKUMENTÓW: do 15 października 2025 r. lub do wyczerpania limitu miejsc.

DOKUMENTY PRZYJMUJE: Uniwersytet Zielonogórski, Sekretariat Wydziału Nauk Inżynieryjno-Technicznych, ul. prof. Z.Szafrana 2, 65-516 Zielona Góra
mgr Katarzyna Szajkowska
Tel: 68 328 25 13, 789 441 819. E-mail: K.Szajkowska@wnit.uz.zgora.pl

CHARAKTERYSTYKA STUDIÓW ORAZ SYLWETKA ABSOLWENTA:
Celem studiów jest przekazanie praktycznej wiedzy w zakresie cyberbezpieczeństwa w kontekście obszaru technicznego, prawnego i zarządczego. Celem studiów jest zdobycie wiedzy i praktycznych umiejętności z zakresu szeroko rozumianego zarządzania cyberbezpieczeństwem: opracowywania strategii cyberbezpieczeństwa, wdrażania procedur bezpieczeństwa, zarządzania ciągłością działania, incydentami cyberbezpieczeństwa oraz ryzykiem. Przekazywana wiedza uwzględnienia zarówno aspekty zapewnienia ochrony infrastruktury teleinformatycznej i systemów, jak i informacji.

- do kogo adresowane:
Studia są adresowane do:

- absolwentów studiów I stopnia, II stopnia lub jednolitych studiów magisterskich, którzy są zainteresowanych zagadnieniami związanymi z cyberbezpieczeństwem i cyberprzestępczością,
- osób, które zajmują się, bądź planują pracę na stanowiskach związanych z prowadzeniem, planowaniem, kontrolowaniem bezpieczeństwa informacji i systemów, w których dane o różnym stopniu poufności są tworzeniem, przesyłane, przetwarzane albo przechowywane,
- administratorów systemów teleinformatycznych, którzy planują pogłębić swoją wiedzę w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji,
- pracowników komórek zarządzania bezpieczeństwem (Security Operations Center, SOC), jak również ekspertów działów IT, audytorów i pentesterów,
- pracowników administracji publicznej, organów ścigania, wymiaru sprawiedliwości, pracowników sektora bankowego i finansowego oraz pracownikom przedsiębiorstw, które zajmują się działaniami w obszarze cyberbezpieczeństwa,
- kadry kierowniczej i zarządzającej odpowiedzialnej za bezpieczeństwo informacji.

- kwalifikacje po ukończeniu studiów:
Absolwenci studiów otrzymają świadectwo ukończenia studiów "Cyberbezpieczeństwo".

Absolwent studiów podyplomowych ma wiedzę z zakresu m.in.: praktycznego stosowania narzędzi oraz technologii związanych z bezpieczeństwem sieci teleinformatycznych w celu zabezpieczania działalności jednostek. Ponadto ma podstawową wiedzę z zakresu funkcjonowania i obsługi rozwiązań zabezpieczających sieci teleinformatyczne. Zna aspekty zarządzania systemami operacyjnymi, które są odporne na ataki. Posiada wiedzę z zakresu stosowanych narzędzi kryptograficznych. Zna zasady wdrażania systemu zarządzania bezpieczeństwem informacji. Ma wiedzę z zakresu regulacji prawnych z obszaru cyberbezpieczeństwa oraz ochrony danych osobowych, jak również struktur systemu cyberbezpieczeństwa w kraju i na świecie. Absolwent studiów zna elementy analizowania systemów teleinformatycznych pod kątem podatności na ataki oraz zasady doboru skutecznego zabezpieczenia systemu przed atakami. Absolwent rozumie zagrożenia związane z cyberbezpieczeństwem w kontekście technologicznym, prawnym i społecznym. Ma świadomość wykorzystywania socjotechniki przez cyberprzestępców. Absolwent studiów podyplomowych jest świadomy stosowania wymagań prawnych związanych z przetwarzaniem danych osobowych w kontekście implementowanych rozwiązań technologicznych i zagrożeń wynikających z braku ochrony prywatności.

INFORMACJE DODATKOWE:
Warunkiem ukończenia studiów podyplomowych jest zaliczenie na ocenę pozytywną wszystkich przedmiotów objętych planem zajęć. Końcowy wynik studiów ustala się na podstawie średniej arytmetycznej wszystkich ocen. Studia realizowane będą w formie hybrydowej.

KIEROWNIK STUDIÓW:
dr inż. Anna Pławiak-Mowna, prof. UZ
Uniwersytet Zielonogórski, Instytut Sterowania i Systemów Informatycznych
ul. prof. Z. Szafrana 2
65-516 Zielona Góra
amowna@uz.zgora.pl