

Dodatkowe zasady rekrutacji na studia podyplomowe

Cyberbezpieczeństwo infrastruktury transportu szynowego

Ze względu na specjalistyczny oraz interdyscyplinarny charakter studiów podyplomowych „Cyberbezpieczeństwo infrastruktury transportu szynowego”, obejmujących zagadnienia z zakresu cyberbezpieczeństwa, systemów sterowania ruchem kolejowym, automatyki przemysłowej, infrastruktury krytycznej, teleinformatyki oraz systemów elektroenergetycznych, Komisja Rekrutacyjna może stosować dodatkowe kryteria kwalifikacyjne, których celem jest zapewnienie odpowiedniego poziomu przygotowania uczestników do realizacji programu kształcenia.

1. Wykształcenie i przygotowanie merytoryczne

Preferowani są kandydaci posiadający dyplom ukończenia studiów wyższych na kierunkach technicznych lub pokrewnych, w szczególności: elektrotechnika, automatyka, informatyka, informatyka techniczna i telekomunikacja, transport, mechatronika, elektronika, energetyka, bezpieczeństwo lub innych kierunkach związanych z projektowaniem, eksploatacją i utrzymaniem systemów technicznych.

Kandydaci legitymujący się ukończeniem innych kierunków studiów mogą zostać zakwalifikowani po pozytywnej ocenie ich dotychczasowego doświadczenia zawodowego oraz kompetencji zdobytych podczas rozmowy kwalifikacyjnej.

2. Rozmowa kwalifikacyjna

Komisja Rekrutacyjna może przeprowadzić rozmowę kwalifikacyjną z kandydatem. Jej celem jest ocena predyspozycji do podjęcia studiów, motywacji do rozwoju zawodowego oraz stopnia przygotowania do realizacji programu kształcenia.

Podczas rozmowy oceniane mogą być w szczególności:

- motywacja do podjęcia studiów oraz planowany sposób wykorzystania zdobytej wiedzy w działalności zawodowej,
- doświadczenie zawodowe związane z transportem szynowym, cyberbezpieczeństwem, automatyką przemysłową, teleinformatyką, energetyką, systemami sterowania lub infrastrukturą krytyczną,
- znajomość podstawowych zagadnień z zakresu sieci komputerowych, systemów operacyjnych, bezpieczeństwa informacji, systemów sterowania przemysłowego oraz infrastruktury kolejowej,
- umiejętność analitycznego myślenia oraz rozwiązywania problemów technicznych,
- znajomość języka angielskiego w zakresie umożliwiającym korzystanie z dokumentacji technicznej i literatury specjalistycznej.

Rozmowa kwalifikacyjna nie ma charakteru egzaminu wiedzy, lecz służy ocenie możliwości efektywnego uczestnictwa w zajęciach oraz ukończenia studiów z pozytywnym wynikiem.

3. Doświadczenie zawodowe

Dodatkowym atutem podczas postępowania kwalifikacyjnego jest doświadczenie zawodowe zdobyte w przedsiębiorstwach lub instytucjach związanych z transportem szynowym, automatyką przemysłową, energetyką, cyberbezpieczeństwem, teleinformatyką, utrzymaniem infrastruktury krytycznej lub nowoczesnymi systemami sterowania.

Szczególnie wysoko oceniane może być doświadczenie zdobyte w przedsiębiorstwach zarządzających infrastrukturą kolejową, u przewoźników kolejowych, producentów taboru i urządzeń sterowania ruchem kolejowym, przedsiębiorstwach energetyki trakcyjnej, operatorach infrastruktury krytycznej, centrach bezpieczeństwa (SOC), zespołach reagowania na incydenty bezpieczeństwa (CERT/CSIRT), przedsiębiorstwach zajmujących się systemami OT (Operational Technology) oraz firmach projektujących i utrzymujących przemysłowe systemy automatyki.

4. Dodatkowe kwalifikacje

W procesie kwalifikacji uwzględniane mogą być również dodatkowe osiągnięcia zawodowe i kompetencje kandydata, w szczególności:

- posiadanie certyfikatów potwierdzających kompetencje z zakresu cyberbezpieczeństwa, bezpieczeństwa informacji, administracji systemami komputerowymi lub sieciami teleinformatycznymi,
- doświadczenie w projektowaniu, konfiguracji lub utrzymaniu systemów informatycznych, sieci komputerowych, systemów przemysłowych oraz systemów sterowania,
- udział w projektach badawczo-rozwojowych lub wdrożeniowych związanych z bezpieczeństwem systemów teleinformatycznych lub infrastruktury krytycznej,
- ukończone szkolenia specjalistyczne oraz udokumentowana aktywność zawodowa w obszarze cyberbezpieczeństwa, automatyki, energetyki lub transportu.

5. Znajomość zagadnień technicznych

Od kandydatów oczekuje się podstawowej orientacji w zagadnieniach obejmujących funkcjonowanie współczesnych systemów teleinformatycznych i automatyki przemysłowej. Dotyczy to w szczególności podstaw działania sieci komputerowych, architektury systemów operacyjnych, zasad bezpieczeństwa informacji, elementów kryptografii, technologii wykorzystywanych w systemach sterowania przemysłowego, sterowników PLC, systemów SCADA oraz podstaw funkcjonowania infrastruktury transportu szynowego.

6. Zadanie problemowe (opcjonalnie)

Komisja Rekrutacyjna może zaproponować kandydatowi krótkie zadanie problemowe odnoszące się do praktycznych aspektów cyberbezpieczeństwa infrastruktury transportowej. Zadanie ma na celu ocenę sposobu analizy problemów technicznych, identyfikacji zagrożeń oraz proponowania działań minimalizujących ryzyko. Nie wymaga ono specjalistycznej wiedzy eksperckiej, lecz pozwala ocenić logiczne myślenie, umiejętność podejmowania decyzji oraz świadomość zagrożeń związanych z funkcjonowaniem infrastruktury krytycznej.

7. Preferowany profil uczestnika

Studia adresowane są przede wszystkim do osób posiadających wykształcenie techniczne oraz zainteresowanych rozwojem kompetencji w zakresie cyberbezpieczeństwa systemów transportu szynowego. Preferowani są kandydaci posiadający doświadczenie zawodowe w sektorze kolejowym, energetycznym, teleinformatycznym, automatyki przemysłowej lub bezpieczeństwa systemów informatycznych. Mile widziane jest również doświadczenie w eksploatacji lub utrzymaniu systemów OT, infrastruktury krytycznej oraz systemów sterowania ruchem kolejowym.

Celem zastosowania dodatkowych kryteriów kwalifikacyjnych jest zapewnienie wysokiego poziomu merytorycznego grupy uczestników, stworzenie warunków do prowadzenia zajęć o zaawansowanym charakterze oraz umożliwienie efektywnej wymiany doświadczeń pomiędzy przedstawicielami środowiska akademickiego i praktykami reprezentującymi sektor transportu szynowego, przemysł oraz operatorów infrastruktury krytycznej.