Dodatkowe zasady rekrutacji na studia podyplomowe

Cyberbezpieczeństwo – praktyczna analiza zagrożeń

Rozmowa kwalifikacyjna to preferowana forma weryfikacji podstawowej wiedzy i umiejętności kandydata na studia podyplomowe Cyberbezpieczeństwo – praktyczna analiza zagrożeń.
Rozmowa kwalifikacyjna ma za zadanie wyłonić tych kandydatów, którzy posiadają wiedzę i umiejętności pozwalające przypuszczać, że kandydat będzie w stanie ukończyć studia podyplomowe z zakresu cyberbezpieczeństwa.

Dla przypomnienia uczestnikiem studiów podyplomowych może być osoba, która posiada kwalifikację pełną co najmniej na poziomie 6 PRK, uzyskaną w systemie szkolnictwa wyższego i nauki (studia pierwszego stopnia, studia drugiego stopnia, jednolite studia magisterskie).
Naturalnymi kandydatami są absolwenci studiów z dyscypliny informatyki technicznej i telekomunikacji oraz informatyki, spełniający wytyczne opisane poniżej.

Idealny kandydat powinien mieć:

- doświadczenie w administracji Linux, Windows w infrastrukturze sieciowej,
- umiejętność pisania skryptów w Linux i Windows,
- wyższe wykształcenie lub wiedzę w zakresie: informatyka, telekomunikacja, inżynieria sieci,
- udokumentowaną wiedza praktyczna (ukończone kursy, certyfikaty, szkolenia),
- umiejętność programowania w języku Python,
- uporządkowaną wiedza w zakresie modelu warstwowym infrastruktury sieciowej,
- wiedzę dotyczącą konfiguracji urządzeń sieciowych,
- podstawową wiedzę z umiejętności technik hakerskich.

Studia umożliwiają również rozwinięcie kompetencji absolwentom innych kierunków studiów, posiadających wiedzę praktyczną z obszaru informatyki. Studia są przeznaczone dla osób posiadających wiedzę informatyczną lub takich, którzy chcieliby taką wiedzę pogłębić, zaktualizować i zdobyć praktyczne umiejętności charakterystyczne dla cyberbezpieczeństwa.