

Bezpieczeństwo systemów teleinformatycznych

STUDIA II STOPNIA - SPECJALNOŚĆ

Forma: Niestacjonarne

Sposób realizacji: Hybrydowe

Cechy: Studia II stopnia • Od października • Polski • 4 semestry

Miasto: Gdańsk



Czego się nauczysz?

- Nauczysz się **identyfikować zagrożenia w sieciach teleinformatycznych**, dzięki czemu będziesz mógł analizować i chronić infrastrukturę IT przed cyberatakami.
- Poznasz **protokoły bezpieczeństwa i metody monitorowania ruchu sieciowego**, co pomoże Ci efektywnie reagować na incydenty i minimalizować ryzyko.
- Opanujesz techniki związane z **inżynierią społeczną i analizą cyfrowych śladów**, co pozwoli Ci na lepsze rozpoznawanie zagrożeń w cyberprzestrzeni.
- Zdobędziesz praktyczną wiedzę o **zintegrowanych systemach zarządzania bezpieczeństwem**, co przygotuje Cię do ochrony danych w organizacjach.
- Nauczysz się wykonywania **testów penetracyjnych oraz skanowania systemów IT**, co pozwoli Ci identyfikować luki w zabezpieczeniach i je eliminować.
- Zrozumiesz zasady **ochrony sieci WiFi i kryptografii współczesnych systemów**, co umożliwi Ci zabezpieczanie poufnych danych i komunikacji.

Praca dla Ciebie

- **Pracuj jako specjalista ds. bezpieczeństwa IT.** Twoim zadaniem będzie monitorowanie sieci, analizowanie zagrożeń i wdrażanie zabezpieczeń w systemach IT.
- **Zostań konsultantem ds. bezpieczeństwa IT**, pomagając firmom identyfikować i eliminować luki w zabezpieczeniach oraz opracowywać strategie ochrony danych.
- **Zatrudnij się jako tester zabezpieczeń IT (Penetration Tester)**, sprawdzając podatność systemów na ataki i rekomendując rozwiązania poprawiające bezpieczeństwo.
- **Bądź menedżerem ds. cyberbezpieczeństwa**, nadzorując zespoły specjalistów, zarządzając polityką bezpieczeństwa i dbając o ochronę infrastruktury informatycznej.
- **Rozwijaj się jako specjalista ds. cyberbezpieczeństwa**, chroniąc organizacje przed cyberprzestępcami, reagując na incydenty i opracowując systemy zarządzania ryzykiem.
- **Pracuj w laboratorium bezpieczeństwa IT**, gdzie wykorzystasz zaawansowane technologie do analizy cyfrowych śladów, testów penetracyjnych i obrony przed cyberatakami.

Program studiów

Praktyczne studia

Uczymy tak, aby jak najlepiej przygotować Cię do rzeczywistych wyzwań, z jakimi spotkasz się w pracy zawodowej.

- **Projekty grupowe** – realne problemy biznesowe.



- **Symulacje** – decyzje w warunkach rynkowych.
- **Staże i praktyki** – doświadczenie w firmach.
- **Wykłady z praktykami** – eksperci z rynku.
- **Nowoczesne narzędzia** – aktualne technologie.
- **Case studies** – analiza realnych przypadków.

Wybrane zajęcia kierunkowe

- Front-end aplikacji webowych
- Tworzenie back-endu do aplikacji webowych
- Programowanie aplikacji webowych z wykorzystaniem platformy .NET
- Programowanie aplikacji webowych w Java
- RIA, Case study: Angular
- Technologie tworzenia stron WWW
- Tworzenie aplikacji PWA
- Programowanie z elementami algorytmiki
- Projektowanie UX i interfejsów użytkownika
- Programowanie w języku Python
- Techniki zapewniania jakości oprogramowania
- Tworzenie aplikacji internetowych i bazodanowych

Wybrane zajęcia specjalnościowe

- Bezpieczeństwo systemów i sieci komputerowych
- Bezpieczeństwo teleinformatyczne
- Bezpieczeństwo usług opartych na chmurze
- Cyberprzestępczość
- Zintegrowane systemy zarządzania bezpieczeństwem
- Zespołowy projekt bezpieczeństwa
- Współczesne protokoły kryptograficzne



Rozwijaj kompetencje językowe na studiach II stopnia

- Podczas studiów realizujesz jeden przedmiot kierunkowy w języku angielskim.
- W 4. semestrze obowiązkowo zrealizujesz przedmiot w języku angielskim, dostosowany do wybranej specjalności.
- Dodatkowo możesz wybrać dwa kolejne przedmioty w tym języku – wykładowy i ćwiczeniowy.
- To świetna okazja, aby rozwijać kompetencje językowe i zdobywać wiedzę w międzynarodowym kontekście.

Praktyki i staże

Praktyki zawodowe to ważny element studiów. Studenci studiów magisterskich realizują **480 godzin praktyk w całym toku studiów**, zdobywając doświadczenie zawodowe. Jeśli pracujesz w zawodzie zgodnym z kierunkiem studiów, możesz zaliczyć praktyki na podstawie zatrudnienia. W trakcie studiów masz też szansę na płatny staż. Programy stażowe przygotowują pracodawcy, z którymi współpracujemy, dostosowując wymagania do stanowisk, co ułatwia pierwsze kroki zawodowe.

To kierunek dla osób, które:

- chcą chronić systemy i sieci przed cyberatakami,
- interesują się kryptografią, testami penetracyjnymi i analizą zagrożeń,
- planują karierę w obszarze cyberbezpieczeństwa i ochrony danych w organizacjach.

Zasady rekrutacji

Aby zostać **studentem studiów II stopnia** na Uniwersytecie WSB Merito, należy:

- ukończyć studia I stopnia (**licencjackie, inżynierskie**) lub **jednolite studia magisterskie**,
- złożyć komplet wymaganych dokumentów,
- spełnić warunki określone w zasadach rekrutacji
- o przyjęciu decyduje kolejność zgłoszeń oraz kompletność dokumentów.

[Dowiedz się więcej](#)

Stypendia i zniżki

- Możesz otrzymać te same stypendia, co studenci uczelni publicznych, w tym naukowe, sportowe, socjalne i zapomogi.
- Elastyczny system opłat pozwala Ci wybrać, w ilu ratach chcesz opłacać czesne.

[Dowiedz się więcej](#)



Ceny

W oparciu o art. 80 ust. 3 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce uczelnia raz w roku akademickim zwiększa wysokość czesnego określonego w § 3 ust. 1 Umowy o wskaźnik równy wskaźnikowi wzrostu cen towarów i usług konsumpcyjnych za rok kalendarzowy poprzedzający rok, w którym dokonuje się waloryzacji, ogłoszony przez Prezesa Głównego Urzędu Statystycznego, łącznie nie więcej niż o 30 % do czasu ukończenia studiów określonych w Umowie.