



Cyberbezpieczeństwo i ochrona zasobów informacyjnych

- Kierunek - studia podyplomowe

Hybrydowe 2 semestry

Opis kierunku

Dwusemestralne studia podyplomowe na kierunku **Cyberbezpieczeństwo i ochrona zasobów informacyjnych** mają na celu poszerzenie i uzupełnienie wiedzy, umiejętności oraz kompetencji w zakresie opracowywania i stosowania szeregu procesów i praktyk w celu ochrony komputerów, danych, sieci i programów przed atakami, uszkodzeniami i nielegalnym dostępem. Studia mają na celu wykształcić ekspertów poszukiwanych na rynku pracy, gdyż wiele organizacji boryka się z problemem znalezienia dedykowanego specjalisty ds. cyberbezpieczeństwa.

Cel studiów

Przygotujemy Cię do pełnienia funkcji specjalisty odpowiedzialnego za szeroko pojęte cyberbezpieczeństwo w podmiotach gospodarczych i nie tylko.

Korzyści

Zostaniesz specjalistą w obszarze cyberbezpieczeństwa z możliwością pełnienia ról doradcy, projektanta, testera oraz analityka.

Jak wynika z wielu badań i publikowanych raportów między innymi pt. „State of Cybersecurity: Implications”, wiele organizacji boryka się z problemem znalezienia dedykowanego specjalisty ds. cyberbezpieczeństwa.

Uzyskasz umiejętność nie tylko zwiększenia odporności firmy na cyberzagrożenia, lecz także zachowanie odpowiedniego balansu z umiejętnością wykrywania ataku i przywróceniem ciągłości działania po wystąpieniu zakłóceń procesów biznesowych nimi spowodowanych

Dla kogo?

Po kierunku cyberbezpieczeństwo będziesz specjalistą w obszarze bezpieczeństwa cybernetycznego, co Pozwoli Tobie na znalezienie zatrudnienia m. in. w takich podmiotach jak:

- Instytucje rządowe.
- Instytucje finansowe, np. banki.
- Linie lotnicze.
- Firmy doradcza w zakresie bezpieczeństwa.
- Każda duża organizacja.

Hybrydowe studia podyplomowe

Około 50% zajęć zrealizujesz na uczelni, a 50% na platformie MS Teams, w czasie których z wykładowcami i kolegami z grupy kontaktujesz się przez internet, w czasie rzeczywistym (synchronicznie). Dodatkowo skorzystasz z materiałów zamieszczanych w Internecie i na platformie Moodle, w dogodnym dla Ciebie czasie (asynchronicznie).

Program studiów

Program studiów podyplomowych na kierunku **Cyberbezpieczeństwo i ochrona zasobów informacyjnych.**



Liczba miesięcy nauki:

9



Liczba godzin: **160**



Liczba zjazdów: **9**



Liczba semestrów: **2**

Prawne aspekty ochrony danych (20 godz.)

Podstawowe zagadnienia ochrony danych w systemach IT: system źródeł prawa krajowego i międzynarodowego, kary pieniężne

Przestępstwa komputerowe

Sankcje karne w cyberprzestępczości

Dyrektywa Parlamentu Europejskiego i Rady (UE) (18 godz.)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii:

Organy właściwe do spraw cyberprzestępstwa
Obowiązki operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych
CSIRT MON, CSIRT NASK i CSIRT GOV – zadania

Ochrona zasobów informacyjnych w praktyce (46 godz.)

Zagrożenia dla bezpieczeństwa w cyberprzestrzeni
Postępowanie wyjaśniające i dochodzenie w przypadku naruszeń bezpieczeństwa systemów IT
Analiza ryzyka i zarządzanie bezpieczeństwem w cyberprzestrzeni
Ochrona danych osobowych w systemach IT (RODO), bezpieczeństwo informacji niejawnych w systemach teleinformatycznych

Informatyczne aspekty cyberbezpieczeństwa (32 godz.)

Bezpieczeństwo sieci komputerowych i telekomunikacyjnych
Bezpieczeństwo systemów i aplikacji
Nowe technologie - cloud computing, Internet of Things – IoT
Open-source intelligence

Zarządzanie jakością ISO/IEC 27032 (36 godz.)

Uwarunkowania normatywne – zarządzanie jakością ISO/IEC 27032
Funkcjonalne systemy bezpieczeństwa – bezpieczeństwo fizyczne i środowiskowe
Reagowanie na incydenty bezpieczeństwa IT
Audyt i kontrola systemów IT

SEMINARIUM (8 godz.)

Seminarium

Forma zaliczenia



Test



Projekt

Wykładowcy

Piotr Robakowski

Ekspert ds. kluczowych projektów i rozwiązań biznesowych. Politolog, od wielu lat jest specjalistą w zakresie bezpieczeństwa informacji a swoją wiedzę przekazuje współpracując z wieloma przedsiębiorstwami oraz prowadząc zajęcia w uczelniach wyższych. Jest osobą solidną w działaniu i komunikatywną, dzięki czemu prowadzone przez niego szkolenia i zajęcia są ciekawe i jasne w przekazie. Główny Specjalista ds. Bezpieczeństwa, Pełnomocnik ds. Ochrony Informacji Niejawnych i Obronności, Asystent w Instytucie Politologii, Wydziału Nauk Społecznych Uniwersytetu Gdańskiego, Wykładowca w Katedrze i Klinice Medycyny Ratunkowej Gdańskiego Uniwersytetu Medycznego.

mgr Dariusz Groth

Ekspert w zakresie bezpieczeństwa, specjalizuje się w obszarze związanym z bezpieczeństwem wewnętrznym oraz bezpieczeństwem informacji, ochrony danych osobowych, jak również systemem antykorupcyjnym. Specjalista w zakresie zwalczania i zapobiegania przestępczości, terroryzmu współczesnego oraz zarządzania kryzysowego. Wykształcenie zdobywał na Akademii Marynarki Wojennej w Gdyni. Wykładowca w Katedrze bezpieczeństwa wewnętrznego Wyższej Szkoły Bankowej w Gdańsku. Doświadczenie zawodowe zdobył pełniąc służbę w Policji jako oficer Wydziału Kryminalnego, posiadał w ten sposób praktyczną znajomość problematyki bezpieczeństwa.

Na co dzień porusza się również w szerokim spektrum zagadnień związanych z bezpieczeństwem jako Inspektor Ochrony Danych Osobowych.

- Audytor wewnętrzny Systemu Zarządzania Działaniami Antykorupcyjnymi wg ISO 37001
- Inspektor Ochrony Danych Osobowych, audytor wewnętrzny systemów zarządzania bezpieczeństwem informacji wg ISO/IEC 27001:2013
- Menadżer ds. Cyberbezpieczeństwa wg ISO/IEC 27032:2012

Autor książek i kilkudziesięciu artykułów w publikacjach krajowych, międzynarodowych a także czynny uczestnik konferencji międzynarodowych związanych z tematyką bezpieczeństwa.

Członek krajowej listy profesjonalnych audytorów i kontrolerów wewnętrznych Polskiego Instytutu Kontroli Wewnętrznej https://www.krajowalista.pl/art_158_2717.html

mgr Klaudia Ołownia

Certyfikowany szkoleniowiec oraz wykładowca akademicki. Ekspert w obszarze bezpieczeństwa morskiego państwa,

bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa. Doktorantka na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej. Autorka i współautorka wielu artykułów z zakresu bezpieczeństwa. Uczestniczka oraz członek komitetów organizacyjnych wielu konferencji naukowych oraz seminariów poświęconych bezpieczeństwu.

Doświadczenie zawodowe:

- Inspektor Ochrony Danych
- Pełnomocnik i Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001:2013;
- Audytor Wewnętrzny Systemu Zarządzania wg ISO 9001:2015
- Audytor Wewnętrzny Systemu Zarządzania wg ISO 22301:2012
- Audytor Wewnętrzny Systemu Zarządzania wg ISO 27043:2016

Pracownik Pomorskiego Biura Inspektorów Ochrony Danych sp. z o.o. w którym na co dzień tworzy dokumentację oraz procedury związane z bezpieczeństwem informacji dla przedsiębiorstw z różnych branż.

Ernest Lichocki

Kmdr por. rez. dr inż. Ernest Lichocki, doktor nauk wojskowych w specjalności zarządzanie bezpieczeństwem. Doktorant Akademii Obrony Narodowej. Emerytowany oficer marynarki wojennej. Posiada podyplomowe wykształcenie wyższe w zakresie bezpieczeństwa informacyjnego. Absolwent akademii Marynarki Wojennej. Doświadczenie zawodowe zdobył głównie pełniąc przez wiele lat szereg stanowisk służbowych związanych z bezpieczeństwem teleinformatycznym i teleinformatycznym w strukturach MON. Posiada uprawnienia związane z bezpieczeństwem teleinformatycznym, w tym z ochroną informacji niejawnych. Ukończył w kraju i zagranicą ponad 20 kursów specjalistycznych związanych z bezpieczeństwem systemów łączności, systemów wspomagania dowodzenia i systemów teleinformatycznych. Autor kilkunastu projektów wdrożonych do resortu MON i MSWiA. Autor i współautor ponad 40 publikacji związanych z bezpieczeństwem teleinformatycznym i bezpieczeństwem Infrastruktury Krytycznej Państwa. Stale aktywny zawodowo, obecnie pracownik firmy zajmującej się technologiami AI. Promotor ponad 30 prac magisterskich i licencjackich.

Zainteresowania naukowe: cyberterrorizm oraz bezpieczeństwo morskie państwa.

Zainteresowania: lotnictwo – instruktor szybowcowy, strzelectwo, historia wojskowości.

Partnerzy kierunku



Special promotion for candidates.

Nie czekaj, załóż Konto Kandydata i zapisz się online na studia.



Zapisując się do 15 sierpnia, zyskujesz 1000 zł:

600 zł zniżki w czesnym, która rozliczana jest przez cały okres studiów,
obniżając proporcjonalnie każdą kolejną opłatę czesnego,

400 zł dzięki zwolnieniu z opłaty wpisowej.

do 15 sierpnia

czesne już od

288 zł ~~338 zł~~

miesięcznie

Ceny dla kandydatów

Studia to inwestycja, która się zwraca

W Wyższej Szkole Bankowej szanujemy Twój czas i pieniądze, dlatego o finansach mówimy otwarcie. Nie mnożymy dodatkowych opłat, nie przemycamy małym druczkiem ukrytych kosztów. U nas wiesz dokładnie, za co płacisz.

Studia podyplomowe to inwestycja, która zwraca się już w ich trakcie w postaci nowych umiejętności i kontaktów, które zaowocują w biznesie. Wybierz studia podyplomowe w WSB i przekonaj się na własnym przykładzie, jak inwestować w siebie, aby czerpać z tego korzyści teraz i w przyszłości.

Niestacjonarne - Gwarantowane czesne stałe

	Rok nauki	Czesne
1 rata	1 rok	5550 zł 6150 zł

	Rok nauki	Czesne
2 raty	1 rok	2775 zł 3075 zł

	Rok nauki	Czesne
10 rat	1 rok	555 zł 615 zł



	Rok nauki	Czesne
12 rat	1 rok	463 zł 513 zł



Ceny dla absolwentów WSB

Niestacjonarne - Gwarantowane czesne stałe

	Rok nauki	Czesne
1 rata	1 rok	5350 zł 6150 zł

	Rok nauki	Czesne
2 raty	1 rok	2675 zł 3075 zł

	Rok nauki	Czesne
10 rat	1 rok	535 zł 615 zł

	Rok nauki	Czesne
12 rat	1 rok	446 zł 513 zł