UNIWERSYTET WSB MERITO OPOLE

Analiza i informatyka śledcza

- Kierunek - studia podyplomowe dla SUM z SP

Opis kierunku

Analiza i informatyka śledcza to odpowiedź na zapotrzebowanie rynku zdominowanego przez elektroniczny obieg dokumentów i wzrost liczby przestępstw popełnianych z użyciem cyfrowych nośników informacji. Pozwala zidentyfikować ryzyko w obszarach zagrożonych oraz zastosować mechanizmy kontrolne oraz przygotować uczestnika do zabezpieczania jednostki przy wykorzystaniu narzędzi informatycznych.

Jeśli jesteś zainteresowany studiami podyplomowymi i chcesz dowiedzieć się więcej, zostaw do siebie kontakt!

Wypełnij formularz, a my skontaktujemy się z Tobą.

ZOSTAW KONTAKT

Co zyskujesz?

- Zajęcia prowadzą praktycy w zakresie informatyki oraz informatyki śledczej mający aktualną wiedzę o sposobach i narzędziach działania osób dokonujących przestępstw z wykorzystaniem technologii informatycznych;
- Zajęcia realizowane są w aktywnej, warsztatowej formie, zaś przekazywane treści są bogato ilustrowane przykładami z praktyki;
- Przyswojona wiedza pozwoli na wdrożenie rozważań dzięki czemu będzie możliwe zapewnienie bezpieczeństwa w jednostce;
- Będziesz przygotowany do przeprowadzania i raportowania analiz śledczych różnych nośników informacji, a także prowadzenia audytów oraz stosowania testów penetracyjnych.

UNIWERSYTET WSB MERITO OPOLE

Dla kogo?

Studia są skierowane do pracowników działów bezpieczeństwa firm i instytucji, osób pracujących w organach śledczych i wymiarze sprawiedliwości oraz ekspertów IT, a także osób prowadzących audyt w tym zakresie, którzy chcą specjalizować się w dziedzinie informatyki śledczej oraz osób, dla których wiedza o wykrywaniu przestępstw komputerowych będzie uzupełnieniem kompetencji zawodowych. Do uczestnictwa w studia zaprasza się również absolwentów studiów wyższych chcących poszerzyć swoją wiedzę oraz chcących nabyć nowe umiejętności.

Praca dla Ciebie

· specjalista w organach śledczych;

· pracownik bezpieczeństwa w wymiarze sprawiedliwości;

· funkcjonariusz w służbach specjalnych;

· audytor bezpieczeństwa;

· pracownik działów bezpieczeństwa firm i Jednostek Sektora Finansów Publicznych.

Program studiów

Program studiów podyplomowych na kierunku analiza i informatyka śledcza w WSB w Opolu.

Liczba miesięcy nauki: **9**

Liczba godzin: **176**

Liczba zjazdów: **11**

Liczba semestrów: **2**

Prawne aspekty informatyki śledczej i IT (24 godz.)

Zdalna forma zajęć.

- Definicje i podstawy prawne retencji danych w Polsce (2 godz.)
- ISP a ICP – definicje, różnice, aspekty praktyczne (4 godz.)
- Obowiązek współpracy z organami ścigania - dobre praktyki (2 godz.)
- Pojęcie i podział przestępstw komputerowych (8 godz.)
- Przeszukanie, zatrzymanie i zabezpieczanie dowodów (4 godz.)

- Biegły i specjalista w informatyce śledczej (4 godz.).

Odzyskiwanie danych (24 godz.)

Zdalna forma zajęć.

- Rodzaje informacji w informatyce śledczej (4 godz.)
- Komputery: budowa, zasada działania, systemy plików (4 godz.)
- Operacje na danych i wielkości w IT (4 godz.)
- Budowa plików- FAT 32, NTFS (8 godz.)
- Odzyskiwanie danych z pamięci flash – dyski SSD, pendrive (4 godz.)

Narzędzia cyberprzestępczości (24 godz.)

Zdalna forma zajęć.

- Charakterystyka cyberprzestępczości (4 godz.)
- Narzędzia cyberprzestepcy (12 godzina)
- Wybrane aspekty przestępczości internetowej i jej zwalczanie (8 godz.)

Informatyka i analityka śledcz (63 godz.)

Tradycyjna forma zajęć.

- Wstęp do informatyki śledczej (12 godz.)
- Analiza artefaktów systemu operacyjnego Windows (4 godz.)
- Analiza śledcza przeglądarek, komunikatorów, słów kluczowych (8 godz.)
- Oprogramowanie do analizy śledczej (8 godz.)
- Analiza śledcza urządzeń mobilnych – telefony, tablet (16 godz.)
- Analizy śledcze zapisów audio i wideo (Video & Audio Forensics) (16 godz.).

Identyfikacja i analiza ryzyka oraz audytowanie (16 godz.)

Zdalna forma zajęć.

- Narzędzia (2 godz.)
- Identyfikacja i analiza ryzyka (4 godz.)
- Audyt (10 godz.

Cyberbiezpieczeństwo (24 godz.)

Zdalna forma zajęć.

- Definicje i podstawowe pojęcia (8 godz.)
- Zasady cyberbezpieczeństwa (16 godz.)

Forma zaliczenia

Test sprawdzający wiedzę i umiejętności oraz przygotowanie projektu.

Wykładowcy

dr Agnieszka Dornfeld-Kmak

Doktor nauk o zarządzaniu, doktor nauk humanistycznych, absolwentka licznych studiów podyplomowych. a od 2004r. certyfikowany audytor Ministerstwa Finansów. Praktyk w zakresie audytu wewnętrznego (Urząd Kontroli Skarbowej, 10 Brygada Logistyczna w Opolu, jednostki samorządu terytorialnego). Posiada wieloletnie doświadczenie w zarządzaniu jako zastępca Dyrektora Izby Administracji Skarbowej w Opolu oraz Zastępca Dyrektora Departamentu w Ministerstwie Finansów. Współautorka książek „Zarządzanie ryzykiem procesów – identyfikacja", „Kontrola zarządcza w jednostkach sektora finansów publicznych" oraz innych publikacji z zakresu zarządzania, kontroli zarządczej oraz audytu wewnętrznego. Zainteresowania badawcze: strategia zarządzania ryzykiem, budżet zadaniowy, kontrola zarządcza, audyt wewnętrzny, zarządzanie bezpieczeństwem.

Marcin Tchórzewski

kierownik Projektu w firmie Q4Net, wcześniej Inżynier systemów CCTV w firmie AAT Holding S.A.. Projektant systemów IT i niskoprądowych. Projekty i wdrożenia systemów IT i systemów bezpieczeństwa w sektorze energetyki (PGE Bogatynia, Turów), obronnym (Jednostki Wojskowe, magazyny), służby więziennej (Zakłady karne i Areszty śledcze), policji, prokuratury, administracji publicznej (Urzędy miast, gmin), zakładów przemysłowych (PPG, NSK, Toyota). Autor artykułów o systemach bezpieczeństwa dla czasopisma „Twierdza". Praktyczne wdrożenia rozbudowanych systemów bezpieczeństwa i IT w wielu miejscach. Audyty instalacji i rozwiązywanie problemów poprawnym działaniem systemów. Wdrażanie i zarzadzanie programami naprawczymi. Uczestnictwo w wykładach i prezentacjach dla sektora energetyki, JW i SW.

Dawid Czerner

Dyrektor zarządzający, dyrektor IT. Absolwent AGH, WSE i UEK na kierunkach "Informatyka stosowana", "Zarządzanie projektami", "Zarządzanie przedsiębiorstwem". Odpowiedzialny za organizację pracy i realizację celów strategicznych agencji. W największych projektach IT przyjmuje również rolę project managera. W pracy wykorzystuje doświadczenie zdobyte na różnych stanowiskach. Łączy wiedzę techniczną z kompetencjami miękkimi skupiając się na celach biznesowych. Od lat młodzieńczych zafascynowany technologiami i marketingiem internetowym.

Małgorzata Godlewska

magister inżynier, absolwentka Wydziału Elektrotechniki i Automatyki Politechniki Opolskiej. Oficer Służby Więziennej, koordynator zespołu informatyków. Praktyk, zajmuje się wdrażaniem nowych technologii w zakresie zasad

gromadzenia, przekazu i przetwarzania informacji, integracją technologii cyfrowych, administrowaniem sieci komputerowych, systemami komputerowymi i bazami danych, a także zapewnieniem bezpieczeństwa przetwarzanych w nich danych. Jej działalność zawodowa obejmuje również pełnienie roli administratora systemu informatycznego do przetwarzania informacji niejawnych, gdzie odpowiada za jego funkcjonowanie oraz przestrzeganie zasad i wymagań bezpieczeństwa. Posiada doświadczenie w prowadzeniu szkoleń obejmujących m.in elektronizację i cyfryzację w administracji publicznej, a także ochronę danych i bezpieczeństwa IT.

Paweł Dornfeld

Praktyk w zakresie informatyki, Funkcjonariusz Służby Więziennej, były nauczycie informatyki, autor wielu publikacji z zakresie aspektów informatycznych i bezpieczeństwa informacji. Organizator i współorganizator wielu szkoleń dotyczących w tematyce informatycznej. Autor lub współautor Ryzyko w systemach informatycznych firm transportowych, Czasopismo Logistyka; Zarządzanie sytuacjami awaryjnymi w odniesieniu do systemów informatycznych w jednostkach sektora finansów publicznych, Zeszyty naukowe WEIZ PO; Identyfikowanie i analiza ryzyka w systemach informatycznych przedsiębiorstw, Zeszyty Naukowe Wydziału Inżynierii Produkcji I Logistyki Politechniki Opolskiej; Ryzyko zagrożeń dla systemów informatycznych przedsiębiorstw cz. 1 i 2 – Czasopismo Logistyka; Zarządzanie ryzykiem informatycznym w organizacji, Optymalizacja struktur procesów wytwórczych, Międzynarodowe Seminarium Naukowe 2013; Logistyka w „kratkę”, Czasopismo Logistyka; Czynniki ryzyka w obszarze procesów przepływu informacji w jednostkach samorządowych – wyniki badań, Zeszyty naukowe Politechniki Śląskiej, Organizacja i Zarządzanie 2017; Szczegółowy obszar zawodowych zainteresowań: informatyka, aspekt zarządzania bezpieczeństwem informacji, bezpieczeństwem.

Aleksander Jakubowski

magister. Od ponad 12 lat pełni funkcję inspektora Administratora Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Białymstoku. Zainteresowania i działania w zakresie: ustanawiania, wdrażania, rozwoju i doskonalenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, analizy ryzyka w bezpieczeństwie informacji (PN-ISO/IEC 27005), analizy BIA – Business Impact Analysis (ISO/TS 22317),ochrony danych osobowych, przygotowania do wprowadzenia i stosowania RODO (Rozporządzenie Parlamentu Europejskiego i Rady UE 2016-679 z dnia 27 kwietnia 2016 r.), zachowania ciągłości działania (ISO 22301), stosowania zabezpieczeń w celu zachowania dostępności, rozliczalności, poufności i integralności informacji, ochrony danych osobowych.