

Trwa nabór na kolejny cykl Studiów Podyplomowych "Ochrona Danych Osobowych"

Zapraszamy na kolejny cykl rocznych Studiów Podyplomowych dla Inspektorów Ochrony Danych - "Ochrona Danych Osobowych" rozpoczynający się od 01.10.2021 r.

Kontakt: tel. 608-550-339, e-mail: u.nowacka@ujd.edu.pl

Studia realizowane są we współpracy Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie z Polskim Instytutem Kontroli Wewnętrznej sp. z o. o. w Warszawie.

| | |
|---|---|
| Wydział: | Nauk Ścisłych, Przyrodniczych i Technicznych |
| Nazwa studiów: | Ochrona Danych Osobowych |
| Dla kogo? | <p>Warunkiem uczestnictwa w studiach podyplomowych Ochrona Danych Osobowych jest legitymowanie się dyplomem ukończenia studiów wyższych co najmniej pierwszego stopnia.</p> <p>Studia przeznaczone są dla osób, które odpowiadają za proces ochrony danych osobowych w sektorze publicznym, jak i prywatnym. Posiadanie danych osobowych nakłada na organizacje (tak jak i na inne podmioty) szereg różnych obowiązków. Są to m.in.:</p> <ol style="list-style-type: none">1. Obowiązek wyznaczenia inspektora ochrony danych - Administrator i podmiot przetwarzający są obowiązani do wyznaczenia inspektora ochrony danych, w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679. <p>Organy i podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych:</p> <ul style="list-style-type: none">• jednostki sektora finansów publicznych;• instytuty badawcze;• Narodowy Bank Polski; <ol style="list-style-type: none">2. Obowiązek informacyjny wobec osób, których dane dotyczą (m.in. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania, okres, przez który dane osobowe będą przechowywane, czy informację o odbiorcach danych);3. Obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, i inne |
| Jakie kwalifikacje/ uprawnienia po studiach? | Po ukończeniu studiów z wynikiem pozytywnym Absolwenci otrzymują: |

| | |
|---------------------------------------|---|
| | <p>1. Świadectwo Ukończenia Studiów Podyplomowych Ochrona Danych Osobowych wydane przez Uniwersytet Humanistyczno-Przyrodniczy im. Jana Długosza w Częstochowie;</p> <p>2. Certyfikat audytora ds. bezpieczeństwa informacji potwierdzający kwalifikacje na stanowisku Inspektora Ochrony Danych (IOD) wydany przez PIKW.</p> <p>3. Prawo wpisu na Krajową Listę Profesjonalnych Audytorów i Kontrolerów Wewnętrznych prowadzoną przez PIKW Sp. z o.o. (http://www.klpaikw.pl/sklad-krajowej-listy-paikw.art_155.html);</p> <p>4. Bezterminowe wsparcie merytoryczne ze strony Rady Programowej PIKW w zakresie czynności wykonywanych na stanowisku Inspektora Ochrony Danych Osobowych (patrz § 9 Regulaminu KLPAiKW) (http://www.klpaikw.pl/regulamin,165.html).</p> |
| Liczba punktów ECTS: | 30 |
| Liczba godzin: | 210 |
| Czy program obejmuje praktyki? | Program nie przewiduje praktyki |
| Skrócony opis oferty | <p>Celem studiów jest przygotowanie słuchaczy do pracy w zakresie ochrony danych osobowych w przedsiębiorstwach oraz instytucjach zgodnie z krajowymi i międzynarodowymi standardami oraz obowiązującymi przepisami prawa.</p> <p>Studia realizowane są we współpracy Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie z Polskim Instytutem Kontroli Wewnętrznej Sp. z o.o. z siedzibą w Warszawie.</p> <p>Analizując potrzeby pod kątem zapewnienia odpowiednio przygotowanej kadry do pełnienia powyższych zadań studia podyplomowe z zakresu ochrony danych osobowych i jednocześnie z zakresu bezpieczeństwa informacji, pozwalają nabyć fachową wiedzę w przedmiotowym zakresie. Uczestnicy studiów otrzymają wiedzę i umiejętności do rzetelnego wykonywania nałożonych na IOD i osób zajmujących się bezpieczeństwem informacji, a nabyta wiedza przyczyni się to do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych w ich jednostkach.</p> <p>Program studiów obejmuje następujące bloki tematyczne:</p> <p>Wprowadzenie do zagadnień związanych z kontrolą systemów informacyjnych i ochroną danych osobowych.</p> <ul style="list-style-type: none"> • Podstawowe definicje i funkcje związane z obszarem bezpieczeństwa informacji i ochrony danych osobowych. |

- Podejście do kontroli i priorytetyzacja zadań kontrolnych w obszarze przetwarzania danych.
- Zasoby organizacji i proces ich kontroli w podejściu praktycznych do wymienionych zabezpieczeń.
- Rola kontroli w przeciwdziałaniu zagrożeniom związanym z obszarem informacyjnym.
- Analiza najbardziej popularnych zagrożeń i podatności związanych z systemami teleinformatycznymi
- Wprowadzenie do standardów, wytycznych, najlepszych praktyk, kodeksów związanych z bezpieczeństwem informacji i ochroną danych osobowych.

Prawne aspekty ochrony danych osobowych

- wprowadzenie do regulacji prawnych Unii Europejskiej oraz prawa krajowego i międzynarodowego po wprowadzenie ogólnego rozporządzenia o ochronie danych (RODO) i nowelizacji innych przepisów związanych z tematyką ochrony danych osobowych,
- Obowiązki nałożone na administratora oraz podmiot przetwarzający,
- Status i rola IOD - uprawnienia i obowiązki w zakresie ochrony danych osobowych,
- Status i zasady działania organów nadzorczych,
- Monitorowanie przestrzegania przepisów w zakresie ochrony danych osobowych przez pracowników i osoby trzecie oraz działania zapewniające w przedmiotowym zakresie
- Konsekwencje wykonywania działań w zakresie szacowania ryzyka związanego z przetwarzaniem danych osobowych.
- Przepisy przeciwko ochronie informacji wynikające z kodeksu karnego.

Planowanie i realizacja kontroli, sprawdzeń i audytów w zakresie związanym z zabezpieczeniem informacji

- Plan roczny i plany strategiczne
- Etapy tworzenia planu audytu

- Identyfikacja obszarów ryzyka
- Analiza ryzyka na potrzeby planowania
- Audyt poza planem
- Realizacja audytu IT - program audytu, techniki gromadzenia dowodów, próbkowanie i dokumentowanie wyników
- Krajowe i międzynarodowe standardy audytu wewnętrznego
- Krajowe i międzynarodowe wytyczne dla Inspektorów ochrony danych osobowych
- Znaczenie audytu IT w organizacji
- Kodeks etyki audytora

Planowanie i organizacja systemów informatycznych służących do przetwarzania danych osobowych

- Plan strategiczny
- Architektura informatyczna i kierunek technologiczny
- Zarządzanie zasobami ludzkimi w IT
- Zarządzanie inwestycjami
- Zarządzanie projektami IT

Zarządzanie ryzykiem w obrębie danych osobowych

- Metodyka zarządzania ryzykiem w zakresie bezpieczeństwa informacji,
- Organizacja i odpowiedzialności w zakresie procesu oceny i szacowania ryzyka,
- Szacowanie ryzyka - warsztaty praktyczne,
- Tworzenie planów postępowania z ryzykiem
- Informowanie o ryzyku,
- Monitoring i przegląd ryzyka.

Inspektor ochrony danych - realizacja zadań ustawowych - warsztaty praktyczne

- Zasady prowadzenia i weryfikacji podstawowych rejestrów.
- Działania nadzorcze i kontrolne związane z udostępnianiem i powierzaniem danych osobowych
- Działania doradcze IOD w obszarze zamówień publicznych oraz zasad weryfikacji podmiotu przetwarzającego.
- Weryfikacja procesu rekrutacyjnego oraz procesów związanych z zatrudnieniem
- Prawne aspekty stosowania monitoringu.

Zagrożenia związane z przetwarzaniem danych osobowych w organizacji i rola IOD w tym zakresie.

Projektowanie i kontrola obszaru bezpieczeństwa fizycznego i środowiskowego

- Ustawa o ochronie osób i mienia
- Pracownicy ochrony, ochrona wewnętrzna, SUFO, koncesjonowane podmioty realizujące usługi z zakresu bezpieczeństwa
- Zagrożenia dla bezpieczeństwa, w zależności od uwarunkowań geograficznych, instytucjonalnych, obiektowych
- Plany a instrukcje ochrony obiektów
- ochrona mienia i osób, pracownik kwalifikowany, ustawa o broni i amunicji
- Ochrona osobista i VIP
- Agencje detektywistyczne w służbie biznesu
- Konwoje i inkaso
- Cash processing we współczesnej firmie
- Technika w służbie bezpieczeństwa: SSWiN, CCTV, KD, RCP, inteligentne budynki
- Współczesne systemy zarządzania i kontroli w logistyce (RFID) oraz nadzór nad personelem
- Bezpieczeństwo pożarowe i BHP

- Archiwizacja i bezpieczeństwo dokumentów fizycznych
- Zasady postępowania w sytuacjach kryzysowych, napad, włamanie, pożar, podłożenie ładunku wybuchowego, z pierwszej pomocy przedmedycznej
- Organizacja kancelarii tajnych i procesu kontroli informacji niejawnych

System zarządzania bezpieczeństwem informacji zgodny z wymaganiami ISO/IEC 27001:2013

- Struktura i podstawy ISMS
- Organizacja bezpieczeństwa
- Bezpieczeństwo zasobów ludzkich
- Zarządzanie aktywami
- Kontrola dostępu
- Kryptografia
- Bezpieczeństwo fizyczne oraz środowiskowe
- Bezpieczna eksploatacja. Zarządzanie sieciami i systemami informatycznymi
- Bezpieczeństwo komunikacji
- Pozyskiwanie, rozwój oraz utrzymanie systemów
- Relacje z dostawcami
- Zarządzanie incydentami
- Aspekty bezpieczeństwa w zarządzaniu ciągłością działania
- Zgodność z przepisami prawa i standardami

Audyt infrastruktury teleinformatycznej

- Techniki przeprowadzania audytu infrastruktury informatycznej,
- Podejście do mobilności i przetwarzania danych w chmurach obliczeniowych;

- Techniki kontroli warstwy sieciowej, systemowej i aplikacyjnej,
- Tworzenie audytowych list kontrolnych: CASE STUDY

Najczęściej występujące niezgodności i problemy identyfikowane w trakcie audytów.

Wykrywanie i zapobieganie oszustwom i nadużyciom skutkującym wyciekami danych osobowych.

- Zajęcia laboratoryjne

Metody analizy podatności i luk w oprogramowaniu, zabezpieczania systemów i struktur IT, bezpieczeństwo sieci bezprzewodowych, zarządzanie backupem, niszczenie i odzyskiwanie danych, analiza materiału dowodowego

Ochrona organizacji przed wyciekami danych osobowych

- Zajęcia laboratoryjne

Wdrażanie i możliwości administracyjne systemów klasy DLP (Data Leakage Prevention/Prevention)

Kontynuacja działalności po awarii. Zarządzanie ciągłością działania

- Role i odpowiedzialności
- Plany awaryjne
- Plany przywracania systemów po awarii
- Testowanie planów awaryjnych

Odtwarzanie techniki teleinformatycznej po katastrofie.

Zarządzanie kryzysowe. Krajowy system cyberbezpieczeństwa.

- Działania w czasie kryzysu.
- Działania lokalnych komórek CSIRT
- Obowiązki operatorów usług kluczowych i dostawców usług cyfrowych
- Organizacja systemu zarządzania cyberbezpieczeństwem

| | |
|---|--|
| | <ul style="list-style-type: none"> • Architektura cyberbezpieczeństwa - określenie i powołanie struktur wewnętrznych <p>Współpraca z sektorowymi zespołami cyberbezpieczeństwa</p> <p>Bezpieczeństwo prawne - rozszerzone podejście</p> <ul style="list-style-type: none"> • Kodeks karny • Przepisy przeciwko ochronie informacji • Odpowiedzialność z tytułu naruszenia przepisów ODO • Analiza projektów i nowelizacji • Prawa autorskie i zasady ochrony własności intelektualnej. • Dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz postępowaniach cywilnych. <p>Tajemnica przedsiębiorstwa i inne tajemnice prawnie chronione.</p> <p>Seminarium dyplomowe (projektowe)</p> |
| Wymogi związane z ukończeniem studiów: | <p>Warunkiem koniecznym ukończenia studiów podyplomowych „Ochrona Danych Osobowych” jest uzyskanie wszystkich założonych efektów kształcenia, z czym wiąże się:</p> <ul style="list-style-type: none"> • Uczestnictwo w zajęciach; • Zaliczenie na ocenę pozytywną wszystkich przedmiotów objętych programem studiów oraz pozytywne oceny ze wszystkich egzaminów przewidzianych w planie studiów; • Przygotowanie pracy końcowej i jej obrona. |
| Warunki otrzymania świadectwa: | <p>Po obronie pracy końcowej absolwenci otrzymują świadectwo ukończenia studiów podyplomowych wydane przez Uniwersytet Humanistyczno-Przyrodniczy im. Jana Długosza w Częstochowie, zgodne z Rozporządzeniem Ministra Pracy i Polityki Socjalnej w sprawie zasad i warunków podnoszenia kwalifikacji zawodowych i wykształcenia ogólnego dorosłych.</p> <p>Ponadto otrzymują certyfikat audytora ds. bezpieczeństwa informacji potwierdzający kwalifikacje na stanowisku IOD wydany przez PIKW Sp. z o.o.</p> |
| Cena za semestr: | 2500 zł |
| Organizacja zajęć: | Studia Podyplomowe „Ochrona Danych Osobowych” są prowadzone zgodnie z Regulaminem Studiów Podyplomowych obowiązującym na Uczelni. Studia trwają dwa semestry, łączny wymiar godzin - 210, |

za każdy semestr słuchacz zdobywa 30 punktów ECTS. Zajęcia prowadzone są w formie zjazdów sobota-niedziela wg zaplanowanego harmonogramu.

W toku studiów słuchacze uzyskują wiedzę, umiejętności i kompetencje społeczne określone poprzez efekty kształcenia. Zajęcia będą prowadzone w postaci wykładów, konwersatoriów i laboratoriów. Wykładowcy stosują nowoczesne formy przekazu. Zajęcia dydaktyczne odbywać się będą w budynku Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie przy Al. Armii Krajowej 13/15. Uczelnia dysponuje odpowiednią bazą dydaktyczną.

Koordinator kierunku:

Stanisław Hady-Głowiak - Audytor II stopnia, wieloletni pracownik administracji publicznej, autor wielu publikacji naukowych, branżowych, doświadczony Inspektor Ochrony Danych, absolwent studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Śląskiego, absolwent studiów podyplomowych z zakresu audytu wewnętrznego na Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego współorganizowanych z PIKW, uczestnik studiów i wizyt studyjnych w ramach programów międzynarodowych, stażysta programu międzynarodowego w korporacji prawnej w Londynie, wykładowca prowadzący szkolenia i kursy oraz wykłady na uczelniach publicznych, ekspert ds. bezpieczeństwa informacji.

Opiekun merytoryczny:

Piotr Błaszczak - od kilkunastu lat ściśle zajmuje się tematyką związaną z bezpieczeństwem informacji. Od kilku lat współpracuje z jednostką certyfikacyjną CIS - Certification Security Services Sp. z o. o. Właściciel firmy LOCOS zajmującej się audytem, wdrożeniami systemów bezpieczeństwa, testami penetracyjnymi i analizą computer forensics. Przez kilkanaście lat pełnił funkcję CSO (Chief Security Officer) w jednej z agencji rządowych, a wcześniej w sektorze bankowym. Obecnie odpowiada za bezpieczeństwo informacji w grupie kapitałowej będącej jednym z największych graczy rynku e-commerce a także w ramach outsourcingu funkcji Inspektora ochrony danych nadzoruje bezpieczeństwo Spółek funkcjonujących w obszarze finansów i płatności mobilnej oraz służby zdrowia. Niezależny konsultant ds. bezpieczeństwa IT, biegły sądowy z zakresu przestępstw przy użyciu sprzętu i sieci komputerowych, audytor systemów IT, CICA (Certified Internal Controls Auditor), CISSO (Certified Information Systems Security Officer), audytor wiodący ISO 27001, ISO 20000, ISO 22301, EN 50600. Uczestnik i koordynator wielu projektów audytowych oraz postępowań kontrolnych realizowanych w organizacjach sektora prywatnego i publicznego. Trener realizujący zadania dla wielu firm z zakresu bezpieczeństwa informacji, audytu teleinformatycznego, danych

| | |
|---|--|
| | <p>osobowych, ochrony własności intelektualnej w sektorze nowych technologii oraz prawnych aspektów umów w IT.</p> <p>Prowadzący:</p> <p>Praktycy, specjaliści z wieloletnim doświadczeniem w zakresie przeprowadzania audytów bezpieczeństwa informacji i systemów informatycznych w sektorze publicznym i prywatnym oraz kadra naukowo-dydaktyczna Uczelni.</p> <p>Na zajęciach, praktycy zajmujący się na co dzień tematyką studiów przedstawiają najlepsze praktyki, zawodowe standardy i regulacje dotyczące pracy IOD. Przedstawiona będzie metodologia prowadzenia zadań audytowych w tym zakresie i zasady ich dokumentowania oraz praktyczne warsztaty oparte na odbytych audytach, sprawdzeniach i kontrolach z zakresu szeroko pojętego bezpieczeństwa informacji i ochrony danych osobowych.</p> <p>Na ćwiczeniach i warsztatach słuchacze kształtować będą umiejętności niezbędne do tworzenia i kontroli zasad bezpieczeństwa informacji i ochrony danych osobowych oraz profesjonalnego planowania, przeprowadzenia zadań audytowych i ich właściwego dokumentowania.</p> |
| <p>Dane kontaktowe:</p> <p>adres, mail, telefon, strona www</p> | <p>dr Urszula Nowacka,</p> <p>Wydział Nauk Ścisłych, Przyrodniczych i Technicznych,</p> <p>Uniwersytet Humanistyczno-Przyrodniczy im Jana Długosza w Częstochowie, 42-200 Częstochowa</p> <p>Aleja Armii Krajowej 13/15, pok. 311</p> <p>tel. 608-550-339</p> <p>u.nowacka@ujd.edu.pl</p> <p>www.ujd.edu.pl</p> |