INSPEKTOR OCHRONY DANYCH OSOBOWYCH – PROGRAM STUDIÓW

L.p.	Nazwa przedmiotu i szczegółowy zakres	Liczba godzin	Prowadzący	Semestr
1.	**Wprowadzenie do zagadnień związanych z kontrolą systemów informacyjnych i ochroną danych osobowych.** • 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.	20	Piotr Błaszczeć	I
2.	**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. • Przestępstwa przeciwko ochronie informacji wynikające z kodeksu karnego.	20	Stanisław Hady Głowiak	I
3.	**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	20	Adam Kuczyński	I

4.	**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	10	Artur Rudy	I
5.	**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.	10	Artur Rudy	I
6.	**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.	20	Stanisław Hady Głowiak	I
7.	**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 uwarunkować 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	20	Jacek Kamosiński	II

	• 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			
8.	**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	30	Piotr Błaszczeć	II
9.	**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.	10	Piotr Błaszczeć	II
10.	**Wykrywanie i zapobieganie oszustwom i nadużyciom skutkującym wyciekiem 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	10	Maciej Kaczyński	II
11.	**Ochrona organizacji przed wyciekiem danych osobowych** • Zajęcia laboratoryjne • Wdrażanie i możliwości administracyjne systemów klasy DLP (Data Leakage Prevention/Prevention)	10	Maciej Kaczyński	II
12.	**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.	10	Adam Kuczyński	II

13.	**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 • Architektura cyberbezpieczeństwa – określenie i powołanie struktur wewnętrznych • Współpraca z sektorowymi zespołami cyberbezpieczeństwa	10	Adam Kuczyński	II II
14.	**Bezpieczeństwo prawne – rozszerzone podejście** • Kodeks karny • Przestępstwa 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. • Tajemnica przedsiębiorstwa i inne tajemnice prawnie chronione.	10	Stanisław Hady Głowiak	II
15.	**Seminarium dyplomowe (projektowe)**	10	Stanisław Hady Głowiak	II
	SUMA godzin	**220**		