CENTRUM STUDIÓW PODYPLOMOWYCH
WYŻSZEJ SZKOŁY INFORMATYKI I ZARZĄDZANIA
Z SIEDZIBĄ W RZESZOWIE

PROGRAM STUDIÓW

ZARZĄDZANIE OCHRONĄ INFORMACJI NIEJAWNYCH I DANYCH OSOBOWYCH

PRZEDMIOT	GODZ.	ZAGADNIENIA
Klasyfikacja informacji prawnie chronionych oraz zasady zarządzania nimi	**8**	• Rodzaje tajemnic prawnie chronionych, tajemnice i etyki zawodowe (podstawy ochrony wynikające z 62 ustaw), • Informacje niejawne – rozpoznawanie informacji, które powinny być utajnione, zasady ochrony na podstawie ustawy o ochronie informacji niejawnych, • Dane osobowe - rozpoznawanie danych osobowych, zasady ochrony na podstawie RODO i ustawy o ochronie danych osobowych • Informacje prawnie chronione – rozpoznawanie informacji i zasady ochrony na podstawie wybranych ustaw, • Obowiązki wynikające z ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2019.1429 t.j. z dnia 2019.07.31), • Obowiązki wynikające z ustawy o ponownym wykorzystaniu informacji sektora publicznego z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz.U.2019.1446 t.j. z dnia 2019.08.02), • Odmowa udostępnienia informacji prawnie chronionej – tryb postępowania, uzasadnienie decyzji, • Odmowa zgody na wykorzystanie informacji prawnie chronionej - tryb postępowania, uzasadnienie decyzji.
Prawo do prywatności i ochrony danych osobowych - regulacje międzynarodowe, europejskie i krajowe	**8**	• Geneza ochrony danych osobowych w Europie i Polsce, • Problematyka ochrony danych osobowych na gruncie poszczególnych gałęzi prawa (konstytucyjnego, karnego, administracyjnego, cywilnego oraz prawa pracy), • Podstawowe akty prawne UE (RODO) i krajowe (ustawa) odnoszące się do przetwarzania danych osobowych, • Prawa do wolności słowa i wyrażania swoich opinii a prawo do ochrony danych osobowych.
Prawne aspekty ochrony danych osobowych	**20**	• Zasady dotyczące przetwarzania danych osobowych (art. 5 RODO), • Podstawy przetwarzania danych osobowych (art. 6 RODO), • Zasady przetwarzania danych wrażliwych (art 9 RODO), • Zasady realizacji obowiązku informacyjnego (art. 12 RODO), • Zasady realizacji praw osób których dane są przetwarzane (art. 16-22 RODO), • Procedura rejestrowania i zgłaszania naruszeń (art. 33 i 34 RODO), • Procedura oceny skutków dla ochrony danych (art 35 i 36 RODO), • Procedura powierzania danych osobowych (art. 28-29 RODO), • Prowadzenie rejestrów (art. 30 RODO), • Zawartość polityki ochrony danych osobowych (art.24, motyw 79, art

		5, 7, 12-22, 25, 28, 29, 32, 33, 35, 39 RODO), • Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych (art 44 -49 RODO).
Organ nadzorczy ds. ochrony danych osobowych, jego status, zadania i uprawnienia	8	• Podstawy prawne funkcjonowania organu nadzorczego ds. Ochrony danych osobowych, • Zadania i uprawnienia organu nadzorczego • Współpraca organu nadzorczego z organami nadzorczymi w innych krajach, wspólne operacje organów nadzorczych.
Podstawowe środki zabezpieczenia danych przetwarzanych w systemach teleinformatycznych	**28**	• Podstawowe atrybuty bezpieczeństwa informacji przetwarzanych przy użyciu systemów teleinformatycznych • Zasady, standardy i dobre praktyki w zakresie bezpieczeństwa przetwarzania danych w systemach teleinformatycznych • Metodologie analizy ryzyka w zakresie bezpieczeństwa danych przetwarzanych w systemach informatycznych. • Dobór technicznych i organizacyjnych środków bezpieczeństwa z uwzględnieniem stanu wiedzy technicznej, zakresu, kontekstu i celu przetwarzania danych a także ryzyka, jakie urzeczywistnienie się istniejących zagrożeń może naruszać prawa i wolności osób, których dane są przetwarzane • Znaczenie sektorowych kodeksów postępowania oraz certyfikacji w zapewnieniu ochrony przetwarzanych danych. • Wykorzystanie normy PN-EN ISO/IEC 27002 dla ustanawiania zasad przetwarzania danych osobowych i wyboru środków bezpieczeństwa teleinformatycznego • Środki kontroli dostępu do danych przetwarzanych w systemach teleinformatycznych • Koncepcje zarządzania bezpieczeństwem według PN-EN ISO/IEC 27001.
Szczególne obowiązki zapewnienia bezpieczeństwa informacyjnego w podmiotach publicznych	**4**	• Obowiązki wynikające z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2019.700 t.j. z dnia 2019.04.16), • Obowiązki wynikające z rozporządzenia o Krajowych Ramach Interoperacyjności z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (§ 20 ust 2, pkt 1-14 KRI).
Osobowe i techniczne aspekty bezpieczeństwa informacji przetwarzanych przy zastosowaniu nowych technologii	**16**	• Ochrona danych w systemach telekomunikacyjnych - usługi geolokalizacyjne • Ochrona danych w systemach wykorzystujących technologię rfid, • Ochrona danych osobowych a internet przedmiotów, • Ochrona danych osobowych w sieciach inteligentnego opomiarowania i zarządzania (smart metering, smart grid), • Ochrona danych osobowych w portalach społecznościowych, • Ochrona danych osobowych a profilowanie użytkownika przy użyciu technologii plików cookies, • Ochrona danych osobowych a wtórne wykorzystywanie danych przy użyciu narzędzi analitycznych typu data mining, data analytics, big data.

Organizacja i zasady działania pionu ochrony oraz kancelarii tajnej	**24**	• Zasady klasyfikowania informacji, klauzule ochrony, okresy ochrony, • Zasady tworzenia stref administracyjnej i bezpieczeństwa – elementy systemu zabezpieczeń, • Zasady lokalizacji kancelarii tajnej i system zabezpieczeń, • Zasady kontroli pracy kancelarii tajnej, • Rodzaje dzienników ewidencyjnych i sposoby ich prowadzenia, • Ewidencja wysyłanej i przyjmowanej korespondencji niejawnej, • Sposoby oznaczania materiałów klauzulami tajności, • Dekretowanie dokumentów, • Praktyczne sposoby wykonywania i opisywania dokumentów niejawnych, • Zasady zapoznawania z dokumentami niejawnymi, • Zasady przewożenia i ochrony dokumentów niejawnych, • Zasady skracania i przedłużania okresów ochrony dokumentów niejawnych • Kancelaria tajna międzynarodowa.
Obowiązki administratorów danych i przetwarzających	**4**	• Rejestracja zbiorów danych jako element wstępnej weryfikacji legalności przetwarzania danych osobowych • Obowiązek prowadzenia rejestry czynności przetwarzania przez administratorów danych oraz przetwarzających • Obowiązek wyznaczenia inspektora ochrony danych oraz powiadomienia o tym organu nadzorczego • Obowiązek rejestrowania naruszeń przetwarzania danych osobowych, ich zgłaszania organowi nadzorczemu oraz w razie potrzeby powiadamiania osób, których bezpieczeństwo danych zostało naruszone. • Obowiązek przeprowadzania oceny skutków dla ochrony danych
Dokumentacja bezpieczeństwa teleinformatycznego przetwarzania danych osobowych oraz informacji niejawnych	**28**	• Polityka bezpieczeństwa przetwarzania danych osobowych – wymagane elementy • Instrukcja zarządzania systemem informatycznym używanym do przetwarzania danych osobowych – wymagane elementy i procedury • Ewidencja osób upoważnionych do przetwarzania danych osobowych i sposób jej prowadzenia • Dokument szczególnych wymagań bezpieczeństwa – dla systemu teleinformatycznego wykorzystywanego do przetwarzania informacji niejawnych • Dokumentacja procedur bezpiecznej eksploatacji systemu teleinformatycznego używanego do przetwarzania informacji niejawnych
Systemy zarządzania w ochronie informacji i danych	**16**	• Krótki przegląd systemów zarządzania jakością • Zakres i wymagania normy PN/EN ISO 27001/IEC 27001 • Praktyczne wdrożenia normy 27001 – wytyczne do wdrożenia zawarte w normie PN-EN ISO/IEC 27002:2017 • Zalecenia wynikające z norm PN-ISO/IEC 29100:2017 oraz ISO/IEC 27134:2017 • Znaczenie kodeksów postępowania oraz proces certyfikacji

Audyt systemu zarządzania bezpieczeństwem informacji	**16**	• Wprowadzenie do procesu audytu – wytyczne ISO 19011:2018, • Zasady audytowania – 7 zasad audytowania, • Audyt wewnętrzny w systemie zarządzania bezpieczeństwem informacji, • Planowanie i program audytu bezpieczeństwa informacji, • Przeprowadzenie audytu, • Przegląd dokumentacji, tworzenie list kontrolnych pytań i kwestionariuszy audytowych, dokumentów wspomagających, • Pozyskiwanie obiektywnych dowodów, • Analiza obserwacji audytowych.
Status i obowiązki inspektorów ochrony danych	**4**	• Powołanie i status inspektora ochrony danych, • Zadania inspektora ochrony danych, • Odpowiedzialność inspektora ochrony danych
Status i obowiązki pełnomocników do spraw ochrony informacji niejawnych	**4**	• Powołanie i status pełnomocników do spraw ochrony informacji niejawnych, • Zadania pełnomocników do spraw ochrony informacji niejawnych, • Odpowiedzialność pełnomocników do spraw ochrony informacji niejawnych.
Razem:	**188**	