AUDYT BEZPIECZEŃSTWA INFORMACJI

BLOKI TEMATYCZNE	ZAGDANIENIA
I. Cyberbezpieczeństwo – wprowadzenie (20 godz.)	1. Podstawowe definicje i funkcje związane z obszarem cyberbezpieczeństwa oraz bezpieczeństwa informacji 2. Analiza najbardziej popularnych zagrożeń i podatności związanych z systemami teleinformatycznymi 3. Podatności związane z obszarem IT 4. Wprowadzenie do testów penetracyjnych
II. Audyt wewnętrzny i metodyka przeprowadzania kontroli w obszarze IT (20 godz.)	1. Planowanie strategiczne 2. Etapy tworzenia planu audytu 3. Identyfikacja obszarów ryzyka 4. Analiza ryzyka na potrzeby planowania 5. Audyt poza planem 6. Realizacja audytu IT – program audytu, techniki gromadzenia dowodów, próbkowanie i dokumentowanie wyników 7. Krajowe i międzynarodowe standardy audytu wewnętrznego 8. Znaczenie audytu IT w organizacji 9. Kodeks etyki audytora
III. Bezpieczne projektowanie systemów IT (20 godz.)	1. Planowanie i organizacja systemów IT 2. Architektura informatyczna i kierunek technologiczny 3. Zarządzanie inwestycjami 4. Zarządzanie projektami IT
IV. Zarządzanie ryzykiem w obszarze cyberbezpieczeństwa (20 godz.)	1. Metodyka zarządzania ryzykiem w zakresie bezpieczeństwa informacji 2. Organizacja i odpowiedzialności w zakresie procesu oceny i szacowania ryzyka, 3. Szacowanie ryzyka – warsztaty praktyczne, 4. Tworzenie planów postępowania z ryzykiem 5. Informowanie o ryzyku, 6. Monitoring i przegląd ryzyka.
V. Normalizacja i standardy międzynarodowe w obszarze bezpieczeństwa informacji, cyberbezpieczeństwa i prywatności (40 godz.)	1. ISO/IEC 27001 2. ISO/IEC 27017 3. ISO/IEC 27018 4. ISO/IEC 27701 5. Inne standardy dziedzinowe 6. Standardy NIST
VI. Kontynuacja działalności po awarii. Zarządzanie ciągłością działania. (8 godz.)	1. Role i odpowiedzialności 2. Plany awaryjne 3. Plany przywracania systemów po awarii

	4. Testowanie planów awaryjnych 5. Odtwarzanie techniki teleinformatycznej po katastrofie
VII. Zarządzanie kryzysowe. **Krajowy system cyberbezpieczeństwa.** **(8 godz.)**	1. Działania w czasie kryzysu. 2. Działania lokalnych komórek CSIRT 3. Obowiązki operatorów usług kluczowych i dostawców usług cyfrowych 4. Organizacja systemu zarządzania cyberbezpieczeństwem 5. Architektura cyberbezpieczeństwa – określenie i powołanie struktur wewnętrznych 6. Współpraca z sektorowymi zespołami cyberbezpieczeństwa
VIII. Audyt infrastruktury teleinformatycznej **(20 godz.)**	1. Techniki przeprowadzania audytu infrastruktury informatycznej, 2. Podejście do mobilności i przetwarzania danych w chmurach obliczeniowych; 3. Techniki kontroli warstwy sieciowej, systemowej i aplikacyjnej, 4. Tworzenie audytowych list kontrolnych: CASE STUDY 5. Najczęściej występujące niezgodności i problemy identyfikowane w trakcie audytów.
IX. Regulacje prawne obejmujące szeroko pojęte bezpieczeństwo informacji, prywatność i cyberbezpieczeństwo	1. Kodeks karny 2. Dyrektywa policyjna 3. Przestępstwa przeciwko ochronie informacji 4. Powiązanie RODO a obszar IT 5. Analiza projektów i nowelizacji przepisów o ochronie danych osobowych oraz obszaru cyberbezpieczeństwa 6. Prawa autorskie i zasady ochrony własności intelektualnej. Krajowe Ramy Interoperacyjności. 7. Dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz postępowaniach cywilnych. 8. Tajemnica przedsiębiorstwa i inne tajemnice prawnie chronione
Łączna liczba godzin dydaktycznych	**196**