1. **Nazwa kierunku: ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI - dla jednostek samorządu terytorialnego**
2. **Czas trwania: 2 semestry/ 160 godz.**
3. **Liczba ECTS:** 30
4. **Cel:** Studia podyplomowe na kierunku Zarządzanie bezpieczeństwem informacji mają na celu kompleksowe przygotowanie uczestników do skutecznego zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego (JST). Program koncentruje się na kluczowych zagadnieniach związanych z ochroną danych osobowych, cyberbezpieczeństwem oraz wdrażaniem i audytowaniem systemów zarządzania zgodnych z międzynarodowymi normami, takimi jak ISO/IEC 27001, ISO 27035, czy ISO 22301. Absolwenci zyskają wiedzę i umiejętności niezbędne do identyfikacji zagrożeń, projektowania strategii bezpieczeństwa, przeciwdziałania cyberprzestępstwom, zarządzania incydentami bezpieczeństwa oraz zapewnienia ciągłości działania organizacji.
5. **Uczestnicy studiów**: Program studiów skierowany jest do specjalistów ds. bezpieczeństwa informacji, administratorów systemów informatycznych, audytorów, kierowników działów IT, inspektorów ochrony danych osobowych, a także osób odpowiedzialnych za zarządzanie ryzykiem i ochronę danych w sektorze prywatnym, publicznym i administracji państwowej. Studia są także odpowiednie dla osób pragnących zdobyć nowe kompetencje w zakresie zarządzania bezpieczeństwem informacji, niezależnie od wcześniejszego wykształcenia.
6. **Szczegółowe efekty kształcenia:**

KIERUNKOWE EFEKTY KSZTAŁCENIA	OPIS KIERUNKOWYCH EFEKTÓW KSZTAŁCENIA
WIEDZA	
ZBI_SP_W01	Absolwenci będą posiadać wiedzę na temat norm i przepisów prawnych dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji w Polsce i Unii Europejskiej.
ZBI _SP_W02	Uczestnicy studiów podyplomowych poznają zaawansowane techniki cyberbezpieczeństwa, w tym przeciwdziałanie cyberprzestępczości oraz procedury zabezpieczania systemów informatycznych, aplikacji i sieci.
ZBI _SP_W03	Absolwenci będą znali metody audytowania oraz wdrażania systemów zarządzania bezpieczeństwem informacji zgodnych z normami ISO/IEC 27001, ISO 27035 oraz zarządzania ryzykiem wg ISO 31000.
UMIEJETNOŚCI	
ZBI _SP_U01	Absolwenci będą potrafili identyfikować zagrożenia związane z bezpieczeństwem informacji oraz wdrażać odpowiednie strategie ochrony danych i zasobów informatycznych organizacji.
ZBI _SP_U02	Uczestnicy studiów podyplomowych będą audytować i testować systemyw informatyczne oraz projektować rozwiązania zabezpieczające w oparciu o najnowsze technologie, w tym rozwiązania chmurowe.
ZBI _SP_U03	Absolwenci będą efektywnie zarządzać incydentami bezpieczeństwa, zgodnie z wytycznymi normy ISO 27035, oraz planować działania zapewniające ciągłość działania organizacji (ISO 22301).
KOMPETENCJE SPOŁECZNE	

ZBI _SP_K01	Uczestnicy studiów podyplomowych zdobędą kompetencje związane z komunikacją i współpracą w zespole ds. bezpieczeństwa informacji oraz będą przygotowani do zarządzania interdyscyplinarnymi zespołami w sytuacjach kryzysowych.
ZBI _SP_K02	Absolwenci nabędą umiejętności podejmowania decyzji w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem aspektów etycznych i odpowiedzialności społecznej.
ZBI _SP_K03	Uczestnicy studiów podyplomowych będą przygotowani do współpracy z organami ścigania oraz innymi instytucjami w zakresie przeciwdziałania cyberprzestępstwom oraz w sytuacjach związanych z naruszeniem ochrony danych.

7. Program kształcenia

Lp.	Nazwa przedmiotu	Semestr	Liczba godzin zajęć	ECTS
1	Wprowadzenie do bezpieczeństwa informacji i ochrony danych osobowych	I,II	4	1
2	Krajowy System Cyberbezpieczeństwa oraz dyrektywa NIS i NIS2	I,II	14	3
3	Ochrona danych osobowych – uwarunkowania prawne w Polsce i w Unii Europejskiej	I,II	14	3
4	Prawnokarne aspekty cyberprzestępczości (KK, UOPAPP, UoO Baz Danych, etc)	I,II	14	3
5	Przestępstwa komputerowe. Identyfikacja i przeciwdziałanie	I,II	8	1
6	Zabezpieczanie sieci, komputerów, systemów informatycznych i aplikacji	I,II	10	2
7	Elementy informatyki śledczej - zabezpieczanie dowodów elektronicznych i składanie zawiadomień o przestępstwach komputerowych	I,II	8	2
8	Testowanie i audytowanie sieci, systemów informatycznych oraz aplikacji	I,II	10	2
9	Biały wywiad internetowy. Poszukiwanie wycieków danych.	I,II	10	2
10	Projektowanie bezpieczeństwa w chmurze	I,II	8	1
11	Zarządzanie i audytowanie bezpieczeństwa informacji zgodnie z normą ISO 27001	I,II	16	3
12	Wdrażanie systemu zarządzania bezpieczeństwem informacji zgodnego ISO/IEC 27001 – praktyczne warsztaty	I,II	8	1
13	Audytowanie wdrożonego systemu zarządzania wg ISO/IEC 27001 – praktyczne warsztaty	I,II	8	1
14	Zarządzanie incydentami bezpieczeństwa informacji (ISO 27035)	I,II	10	2

15	Zarządzanie ciągłością działania organizacji (ISO 22301)	I,II	10	2
16	Zarządzanie ryzykiem wg norm ISO 31000, ISO 27005 – praktyczne warsztaty	I,II	8	1

8. Sposób zaliczenia studiów:

po I semestrze nauki – test zaliczeniowy,
po II semestrze nauki – test zaliczeniowy