



**WARSZAWSKA SZKOŁA ZARZĄDZANIA
SZKOŁA WYŻSZA**

ul. Siedmiogrodzka 3A

01-204 Warszawa

Tel. 022 862 32 24

e-mail: manage@wsz-sw.edu.pl

www.wsz-sw.edu.pl

**STUDIA PODYPLOMOWE OCHRONY INFORMACJI
NIEJAWNYCH I DANYCH OSOBOWYCH**

Warszawska Szkoła Zarządzania-Szkoła Wyższa oferuje Podyplomowe Studia Ochrony Informacji Niejawnych i Danych Osobowych. Celem studiów jest przekazanie wiedzy w zakresie profesjonalnej ochrony informacji niejawnych i danych osobowych w oparciu o doświadczenia krajowe i zagraniczne. Oferowane przez nas Studia przeznaczone są dla osób kierujących w instytucjach cywilnych i wojskowych, przedsiębiorstwach i jednostkach wojskowych pionami ochrony informacji niejawnych i danych osobowych, dla osób pracujących w tych pionach lub zamierzających podjąć w nich pracę.

Zajęcia realizowane będą w formie wykładów, ćwiczeń i konwersatoriów. Program studiów obejmuje wiedzę dotyczącą prawnych aspektów ochrony informacji niejawnych i danych osobowych, funkcjonowania i zadań instytucji odpowiedzialnych za ochronę informacji niejawnych i danych osobowych, bezpieczeństwa osobowego, bezpieczeństwa w systemach i sieciach teleinformatycznych oraz uprawnień do korzystania z informacji niejawnych i danych osobowych.

Studia ukierunkowane będą na rozwiązywanie praktycznych problemów i prowadzone będą głównie przez praktyków z tej dziedziny. W ich trakcie kształcimy umiejętności związane z opanowaniem sposobów i stosowaniem procedur ochrony informacji niejawnych i danych osobowych, a także z nadzorem i kontrolą przestrzegania przepisów z zakresu ochrony informacji niejawnych i danych osobowych. W trakcie studiów słuchacze będą m.in.

wykonywać projekty ochrony fizycznej jednostki organizacyjnej oraz poznawać tajniki pracy pełnomocnika ochrony informacji niejawnych, danych osobowych i kancelarii oraz administratora sieci teleinformatycznych.

Studia trwają dwa semestry, a zajęcia odbywają się w trybie zaocznym, w piątki od godz.16.15 do 20.15 oraz w soboty od godz. 9.00 do 17.00 co dwa tygodnie. Zajęcia odbywają się w Warszawie w siedzibie uczelni przy ul. Siedmiogrodzkiej 3 A. Czesne za całe Studia wynosi 2900 zł, istnieje możliwość jego rozłożenia na cztery raty.

Szczegółowych informacji udzielają: kierownik studiów podyplomowych *prof. dr hab. Paweł Soroka* – tel. (22) 862-33-37; e-mail:pawel.soroka@wsz-sw.edu.pl i Koordynator ds. studiów podyplomowych *Elżbieta Woźniakowska* – Tel 022 862 33 40 e-mail: elzbieta.wozniakowska@wsz-sw.edu.pl

Szczegółowy program studiów obejmuje następujące przedmioty i zagadnienia w ilości **208 godzin zajęć**:

- I. **System ochrony informacji niejawnych w RP.** /20 godz/.
 1. Organizacja ochrony informacji niejawnych.
 2. Służby ochrony państwa.
 3. Służby współdziałające.
 4. Rola i zadania kierownika jednostki organizacyjnej.
 5. Zadania i uprawnienia pełnomocnika ochrony.
 6. Podstawowe zadania Pionu Ochrony.
 7. Zadania kierowników jednostek organizacyjnych i pełnomocników ochrony w aktach prawnych.
 8. Kodeks Karny a ochrona informacji niejawnych.

- II. **Bezpieczeństwo osobowe.** /30 godz/.
 1. Wiadomości ogólne.
 2. Udostępnianie informacji niejawnych.
 3. Poświadczenie bezpieczeństwa.
 4. Podmioty uprawnione do prowadzenia postępowań sprawdzających i wydania poświadczenia bezpieczeństwa.
 5. Rodzaje postępowań sprawdzających.
 6. Podstawowe dokumenty przy przeprowadzaniu zwykłego postępowania sprawdzającego.
 - 6.1. Pisemne polecenie kierownika jednostki organizacyjnej (wniosek) o wszczęcie postępowania sprawdzającego.

- 6.2. Ankieta bezpieczeństwa osobowego (wypełnianie ankiety do wszystkich poziomów dostępu).
- 6.3. Zapytanie o udzielenie informacji o osobie.
- 6.4. Prośba o sprawdzenie w kartotece skazanych i tymczasowo aresztowanych.
- 6.5. Wniosek o przeprowadzenie sprawdzeń w ewidencji i kartotekach powszechnie niedostępnych.
- 6.6. Czynności końcowe w postępowaniu sprawdzającym.
- 7. Wydawanie certyfikatów bezpieczeństwa.
- 8. Przykład wypełnienia Ankiety Bezpieczeństwa Osobowego.

III. **Szkolenie w zakresie ochrony informacji niejawnych.** /10 godz/.

IV. **Ochrona informacji niejawnych w NATO i w Unii Europejskiej** /5 godz/.

V. **Bezpieczeństwo teleinformatyczne.** /30 godz/.

- 1. Informacje ogólne.
- 2. Osoby funkcyjne odpowiedzialne za bezpieczeństwo teleinformatyczne.
- 3. Zasady bezpieczeństwa teleinformatycznego.
- 4. Czynniki bezpieczeństwa wpływające na bezpieczeństwo teleinformatyczne.
 - 4.1. Bezpieczeństwo fizyczne systemów i sieci teleinformatycznych.
 - 4.2. Bezpieczeństwo osobowe.
 - 4.3. Bezpieczeństwo sprzętowe.
 - 4.4. Ochrona kryptograficzna.
 - 4.5. Bezpieczeństwo transmisji.
- 5. Kontrola dostępu do systemu lub sieci teleinformatycznych.
 - 5.1. Wymagania w zakresie haseł.
- 6. Dokumentacja w zakresie bezpieczeństwa teleinformatycznego.
- 7. Dopuszczenie systemów i sieci do przetwarzania informacji niejawnych .
- 8. Kontrole bezpieczeństwa.
- 9. Bezpieczeństwo informacji.
- 10. Przenośne systemy teleinformatyczne.
- 11. Oprogramowanie złośliwe i wirusy.
- 12. Wykrywanie „kodów złośliwych”

VI. **Ochrona fizyczna informacji niejawnych.** /20 godz/.

- 1. Informacje ogólne.

2. Cel stosowania środków ochrony fizycznej.
3. Strefy bezpieczeństwa.
4. Plan ochrony.

VII. **Kontrole z zakresu ochrony informacji niejawnych.** /10 godz/.

1. Postanowienia ogólne.
2. Cele i etapy działań kontrolnych.
3. Kontrole z zakresu ochrony informacji niejawnych.

VIII. **Kancelaria tajna i wykonywanie dokumentów niejawnych.** /25 godz/.

1. Zasady organizacji kancelarii tajnej.
2. Oznaczanie materiałów niejawnych.
3. Postępowanie z dokumentami pochodzącymi z wymiany międzynarodowej.
4. Środki ewidencyjne kancelarii tajnej.
5. Typowe zasady postępowania z dokumentami niejawnymi.
6. Ekspedycja przesyłek niejawnych.
7. Zasady kompletowania dokumentów.
8. Przechowywanie dokumentacji niejawnej.
9. O czym wykonawca powinien pamiętać.
10. Typowe sposoby załatwiania spraw służbowych.

IX. **Akty prawne regulujące problematykę ochrony informacji niejawnych.** /5 godz.

X. **System ochrony danych osobowych** /40 godz/.

1. Zasady przetwarzania danych osobowych.
2. Prawa osób, których dane przetwarza instytucja.
3. Zasady udostępniania danych.
4. Wybrane obowiązki i odpowiedzialność ADO i ABI.
5. Gromadzenie danych do zbiorów danych osobowych.
6. Obowiązek rejestracji zbiorów danych osobowych.
7. Dane wrażliwe – dopuszczalność przetwarzania.
8. Powierzenie przetwarzania danych osobowych.
9. Zabezpieczenie zbiorów danych – przepisy i standardy, metody zabezpieczenia, monitorowanie wdrożonych środków bezpieczeństwa.
10. Prowadzenie ewidencji i rejestrów.

11. Opracowanie i wdrożenie polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym.
12. Opracowanie wniosku zgłoszenia zbiorów danych osobowych do GIODO.
13. Zagrożenia dla ochrony danych osobowych i prawa do prywatności w świetle nowoczesnych technologii biometrycznych i RFID
14. Specyfika wykonania obowiązków zabezpieczenia technicznego i organizacyjnego danych osobowych.
15. Rola i zadania Głównego Inspektora Danych Osobowych.

XI. **Media i prasoznawstwo** **/5 godz/.**

XII. **Seminarium dyplomowe** **/ 8 godz/.**