

## KURS: OCHRONA INFORMACJI NIEJAWNYCH W JEDNOSTCE. PRZETWARZANIE INFORMACJI NIEJAWNYCH, ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO. BEZPIECZEŃSTWO TELEINFORMATYCZNE



### CELE I KORZYŚCI

- **Dostarczenie kompleksowej wiedzy z zakresu ochrony informacji niejawnych, w szczególności dotyczących przetwarzania informacji niejawnych, środków bezpieczeństwa fizycznego oraz teleinformatycznego.**  
Nabycie praktycznych umiejętności dotyczących stosowania przepisów o ochronie informacji niejawnych także w systemach i sieciach teleinformatycznych
- **Omówienie obowiązków informacyjnych kierownika jednostki oraz pełnomocnika ochrony, współpracy, podziału zadań.**
- **Podniesienie wiedzy w zakresie zastosowania wymagań, które są określone w ustawie o ochronie informacji niejawnych i wprowadzenia ich w życie w administracji publicznej, na przykładzie konkretnych rozwiązań, praktycznych przykładów i wzorów.**
- **Nabycie przez uczestników umiejętności opracowania dokumentacji wymaganej ustawą o ochronie informacji niejawnych.**
- **Prezentacja praktycznych zagadnień związanych z przetwarzaniem informacji niejawnych i stosowaniem środków bezpieczeństwa fizycznego w celu ich ochrony oraz bezpieczeństwa przemysłowego, tak, aby skutecznie zabezpieczyć posiadane informacje niejawne, racjonalnie gospodarując przy tym środkami finansowymi.**
- **Prezentowanie problematyki dotyczącej akredytacji systemów teleinformatycznych służących do przetwarzania informacji niejawnych, prowadzenia dokumentacji bezpieczeństwa teleinformatycznego.**
- **Prezentacja analizy ryzyka oraz zarządzania ryzykiem w zakresie przetwarzania informacji niejawnych, procedur kontrolnych w bezpieczeństwie teleinformatycznym.**
- **Możliwość konsultacji kwestii problemowych z ekspertami i innymi uczestnikami.**

### WAŻNE INFORMACJE O KURSIE:

Polecamy Państwu uczestnictwo w 3 dniowym kursie z zakresu ochrony informacji niejawnych w jednostce. Podczas kursu eksperci–praktycy, w sposób przejrzysty kompleksowo omówią regulacje dotyczące właściwej organizacji pracy kancelarii materiałów niejawnych, ewidencji dokumentów oraz zasad przechowywania i ich archiwizacji. Ponadto zostanie przedstawiona problematyka kontroli prowadzonych przez ABW.

Udział w kursie gwarantuje zdobycie czy usystematyzowanie niezbędnej wiedzy z zakresu ochrony informacji niejawnych, bezpieczeństwa teleinformatycznego w jednostce, zarządzania ryzykiem w zakresie OIN. Jest doskonałą okazją do poznania tej niełatwej materii, zarówno od strony teoretycznej, jak i praktycznej.

Zespół prowadzący kurs to dwóch praktyków, byłych pracowników ABW, Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji biegłych w tematyce informacji niejawnych.



**DZIEŃ I. 8 września – NAJWAŻNIEJSZE INFORMACJE Z ZAKRESU OCHRONY INFORMACJI NIEJAWNYCH:**

1. Tajemnice prawnie chronione w Polsce.
2. Aktualne podstawy prawne ochrony informacji niejawnych - przepisy ogólne i resortowe.
3. Podstawowe zasady ochrony informacji niejawnych.
4. Nadzór nad systemem ochrony informacji niejawnych w Polsce:
  - Kolegium ds. Służb Specjalnych,
  - Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego.
5. Ochrona informacji niejawnych w jednostkach organizacyjnych – kierownik jednostki organizacyjnej i pełnomocnik ds. ochrony informacji niejawnych (podział ról i zadań).
6. Pion ochrony w jednostce organizacyjnej – struktura i wymagania wobec personelu.
7. Dokumentacja ochrony informacji niejawnych:
  - ocena poziomu zagrożeń,
  - instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „Zastrzeżone” oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony,
  - instrukcja przetwarzania informacji niejawnych o klauzuli „Poufne”,
  - plan ochrony informacji niejawnych,
  - dokumentacja Pełnomocnika Ochrony.
8. Szkolenia z zakresu ochrony informacji niejawnych.
9. Bezpieczeństwo osobowe – zasady dostępu do informacji niejawnych:
  - upoważnienia do klauzuli „Zastrzeżone”,
  - postępowania sprawdzające - zwykłe i poszerzone,
  - teczki akt postępowania sprawdzających – zawartość, przechowywanie i udostępnianie.
10. Obowiązki informacyjne Kierownika Jednostki Organizacyjnej i Pełnomocnika Ochrony. Karty informacyjne.

**Dzień II. 9 września - PRAKTYCZNE ZAGADNIENIA ZWIĄZANE Z PRZETWARZANIEM INFORMACJI NIEJAWNYCH I STOSOWANIEM ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO W CELU ICH OCHRONY. BEZPIECZEŃSTWO PRZEMYSŁOWE**

1. Ochrona informacji niejawnych w stosunkach międzynarodowych. Krajowa Władza Bezpieczeństwa.
2. System kancelarii tajnych oraz kancelarii tajnych międzynarodowych.
3. Organizacja obiegu materiałów niejawnych na poziomie klauzuli „Poufne” i „Zastrzeżone”.
4. Zasady prowadzenia ewidencji i urządzeń kancelaryjnych.
5. Klasyfikowanie informacji niejawnych. Okresy ochronne.
6. Archiwizacja i brakowanie materiałów niejawnych.
7. Zasady punktacji środków bezpieczeństwa fizycznego. Normy mające zastosowanie przy ochronie informacji niejawnych.
8. Omówienie typowych środków bezpieczeństwa stosowanych do ochrony informacji niejawnych:
  - strefy ochronne,
  - szafy metalowe i meble biurowe,
  - pomieszczenia oraz zamki, ściany i stropy, drzwi i okna,
  - budynki,
  - System Kontroli Dostępu,
  - personel bezpieczeństwa (pion ochrony, firma ochroniarska),
  - System Sygnalizacji Włamania i Napadu,
  - monitoring wizyjny,
  - ogrodzenie i oświetlenie terenu.
9. Certyfikacja środków bezpieczeństwa fizycznego.
10. Zasady dostępu do informacji niejawnych przez przedsiębiorców.
11. Kwestionariusz bezpieczeństwa przemysłowego.
12. Świadectwa bezpieczeństwa przemysłowego – rodzaje i terminy ważności.

13. Podstawowe wymagania związane z zawieraniem z przedsiębiorcami umów, których realizacja wiąże się z dostępem do informacji niejawnych.
14. RODO a ochrona informacji niejawnych.
15. Informacje niejawne a prawo dostępu do informacji publicznej.
16. Informacje niejawne a ochrona danych osobowych.

### Dzień III. 10 września- BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. **Przetwarzanie informacji niejawnych w systemach i sieciach teleinformatycznych. Zasady ogólne.**
2. **Personel bezpieczeństwa.** Administrator systemu i Inspektor Bezpieczeństwa Teleinformatycznego – wymagania formalne, rola i zadania.
3. **Akredytacja systemów teleinformatycznych służących do przetwarzania informacji niejawnych.**
4. **Dokumentacja bezpieczeństwa teleinformatycznego:**
  - szczególne Wymagania Bezpieczeństwa Systemu,
  - procedury Bezpiecznej Eksploatacji.
5. **Analiza ryzyka oraz zarządzanie ryzykiem związanym z przetwarzaniem informacji niejawnych.**
6. **Kryptografia i środki ochrony elektromagnetycznej.**
7. **Środki bezpieczeństwa fizycznego stosowane w celu ochrony systemów i sieci przetwarzających informacje niejawne.**
8. **Sprzętowa Strefa Ochrony Elektromagnetycznej.**
9. **Procedury kontrolne w bezpieczeństwie teleinformatycznym.**
10. **Podstawy konfiguracji BIOS i systemu operacyjnego Microsoft Windows 10 Professional w systemie teleinformatycznym przetwarzającym informacje niejawne.**
11. **Brakowanie nośników informatycznych służących do przetwarzania materiałów niejawnych.**
12. **Podsumowanie kursu. Odpowiedzi na pytania uczestników.**

#### **ADRESACI** >

kierownicy jednostek administracji publicznej, w tym samorządowej, sekretarze w jednostkach samorządu terytorialnego, pełnomocnicy ds. ochrony informacji niejawnych, osoby odpowiedzialne za rejestrację i obieg dokumentów niejawnych, kierownicy Kancelarii Materiałów Niejawnych, pracownicy komórek zarządzania kryzysowego i OC, pracownicy komórek organizacyjnych odpowiedzialnych w jednostce za ochronę informacji niejawnych.

#### **PROWADZĄCY** >

**Prowadzący 1** Absolwent UMK w Toruniu oraz studiów podyplomowych WSAiB w Gdyni na kierunku zarządzanie bezpieczeństwem informacji, certyfikowany Inspektor Ochrony Danych, Menedżer Bezpieczeństwa Informacji oraz Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji. W latach 1992 - 2013 funkcjonariusz UOP/ABW, od 1999r. zajmuje się problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009r. ekspert ABW z zakresu OIN. Współorganizator szkoleń i konferencji poświęconych problematyce ochrony informacji oraz danych osobowych. W latach 2013 - 2017 Pełnomocnik ds. ochrony informacji niejawnych w urzędzie wojewódzkim oraz innych jednostkach.

**Prowadzący 2** Absolwent Wojskowej Akademii Technicznej w Warszawie, studiów podyplomowych z zakresu bezpieczeństwa teleinformatycznego, posiada Certyfikat Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji, ma wieloletnie doświadczenie pracy w pionie ochrony informacji niejawnych na stanowiskach: inspektor BTI oraz administrator systemów TI przetwarzających informacje niejawne w administracji publicznej. W latach 2002 -2006 pracownik ABW na stanowisku kierowniczym w pionie bezpieczeństwa teleinformatycznego; odpowiedzialny m.in. za organizowanie i prowadzenie szkoleń z zakresu bezpieczeństwa TI, posiada doświadczenie w opracowywaniu dokumentacji bezpieczeństwa dla systemów TI przetwarzających informacje niejawne i administrowanie takim systemem.

## INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

**KURS: Ochrona informacji niejawnych w jednostce. Przetwarzanie informacji niejawnych, środki bezpieczeństwa fizycznego. Bezpieczeństwo teleinformatyczne**



Kurs będziemy realizowali w formie webinarium on line.



**8,9,10 września 2021r.** Kurs każdego dnia w godzinach 9:30-14:00



**Cena: 835 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

**CENA zawiera:** udział w profesjonalnym szkoleniu on-line,  
materiały szkoleniowe w wersji elektronicznej,  
certyfikat ukończenia szkolenia,  
możliwość konsultacji z trenerem.

### DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej Podlaskie Centrum  
ul. Choroszczańska 31, 15-732 Białystok  
tel.: 85 732 17 88 | fax: 85 732 94 84  
[frdl-pc@frdl.bialystok.pl](mailto:frdl-pc@frdl.bialystok.pl)

### DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy  
(dane do faktury)

Nazwa i adres odbiorcy

NIP

Telefon

1. Imię i nazwisko uczestnika,  
stanowisko,  
E-MAIL i TEL. DO KONTAKTU

2. Imię i nazwisko uczestnika,  
stanowisko,  
E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe) TAK  NIE

Proszę o certyfikat w formie: Papierowej   
Elektronicznej  e mail.....

Proszę o przesłanie faktury na adres mailowy: .....

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora [www.frdl.bialystok.pl](http://www.frdl.bialystok.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przestać poprzez formularz zgłoszenia na [www.frdl.bialystok.pl](http://www.frdl.bialystok.pl) lub mailem na adres [frdl-pc@frdl.bialystok.pl](mailto:frdl-pc@frdl.bialystok.pl) do 3 września 2021 r.

**UWAGA** Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej \_\_\_\_\_