



Krajowe
Stowarzyszenie
Ochrony Informacji
Niejawnych

Brak ocen dla tego dostawcy

Warsztaty dla administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego. Szacowanie i zarządzanie ryzykiem – proces analizy i oceny ryzyka. Zasady opracowania dokumentacji bezpieczeństwa. Opracowanie Szczególnych Wymagań Bezpieczeństwa (SWB) i Procedur Bezpiecznej Eksploatacji (PBE).

Numer usługi 2026/04/16/8548/3493267

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- 20:00 h
- 22.06.2026 do 24.06.2026

2 337,00 PLN brutto
1 900,00 PLN netto
116,85 PLN brutto/h
95,00 PLN netto/h
126,98 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Prawo i administracja / Ochrona informacji niejawnych

Grupa docelowa usługi

Warsztaty skierowane są zwłaszcza do administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego, dyrektorów i kierowników działów IT, pełnomocników ochrony, a w szczególności tych, którzy zamierzają ubiegać się o akredytację oraz stoją przed problemem stworzenia dokumentacji bezpieczeństwa TI, a także pozostałych pracowników pionów ochrony chcących uporządkować wiedzę i nabyć praktycznych umiejętności przygotowania warunków, opracowania dokumentów oraz wdrożenia systemowych rozwiązań bezpieczeństwa teleinformatycznego. Podczas zajęć omówione zostaną m.in. wprowadzone zmiany w ustawie o ochronie informacji niejawnych dotyczące oznakowania i rejestracji środków ochrony elektromagnetycznej oraz szacowanie ryzyka dla bezpieczeństwa przetwarzanych informacji niejawnych i zarządzanie tym ryzykiem.

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

25

Data zakończenia rekrutacji

18-06-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

20

Cel

Cel edukacyjny

Warsztaty adresowane są zwłaszcza do aktualnych kierowników i pracowników kancelarii tajnych i niejawnych międzynarodowych chcących uaktualnić i poszerzyć swoją wiedzę oraz umiejętności praktyczne.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zna zagadnienia dotyczące stworzenia dokumentacji bezpieczeństwa TI, posiada wiedzę i praktyczne umiejętności przygotowania warunków, opracowania dokumentów oraz wdrożenia systemowych rozwiązań bezpieczeństwa teleinformatycznego.	Udział w zajęciach teoretycznych i praktycznych, ćwiczeniach, wykonywanie ćwiczeń i analiz.	Debata swobodna
		Obserwacja w warunkach rzeczywistych
		Debata swobodna

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Warsztaty dla administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego, w tym nt. szacowania i zarządzania ryzykiem – proces analizy i oceny ryzyka

Warsztaty skierowane są zwłaszcza do administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego, dyrektorów i kierowników działów IT, pełnomocników ochrony, a w szczególności tych, którzy zamierzają ubiegać się o akredytację oraz stoją przed problemem stworzenia dokumentacji bezpieczeństwa TI, a także pozostałych pracowników pionów ochrony chcących uporządkować wiedzę i nabyć praktycznych umiejętności przygotowania warunków, opracowania dokumentów oraz wdrożenia systemowych rozwiązań bezpieczeństwa teleinformatycznego. Podczas zajęć omówione zostaną m.in. wprowadzone zmiany w ustawie o ochronie informacji niejawnych dotyczące oznakowania i rejestracji środków ochrony elektromagnetycznej oraz szacowanie ryzyka dla bezpieczeństwa przetwarzanych informacji niejawnych i zarządzanie tym ryzykiem.

PLAN RAMOWY

- Prawne aspekty ochrony informacji w systemach teleinformatycznych. Ogólne zasady organizacji systemu TI.
- Bezpieczeństwo osobowe; Bezpieczeństwo fizyczne; Bezpieczeństwo elektromagnetyczne; Bezpieczeństwo kryptograficzne; Kontrola dostępu. Zakres obowiązków personelu bezpieczeństwa teleinformatycznego; obowiązki kierownika jednostki organizacyjnej oraz pełnomocnika ochrony; obowiązki IBTI oraz Administratora systemu.
- Bezpieczeństwo teleinformatyczne. Przebieg akredytacji systemu TI: etap planowania; etap projektowania; etap wdrażania; etap eksploatacji; etap wycofywania.
- Bezpieczeństwo teleinformatyczne. Zasady organizacji wynikające z rozporządzenia PRM z 20 lipca 2011 w sprawie wymagań BTI.
- Zasady opracowania dokumentacji bezpieczeństwa. Opracowanie Szczególnych Wymagań Bezpieczeństwa (SWB) i Procedur Bezpiecznej Eksploatacji (PBE).
- Zarządzanie konfiguracją i zabezpieczeniami systemu lub sieci teleinformatycznej. Zasady organizacji i funkcjonowania systemu reagowania na incydenty komputerowe.
- Wybrane aspekty zarządzania ryzykiem w systemach TI: Analiza Poziomu Zagrożeń; Szacowanie Ryzyka.
- Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle ustawy z dnia 5 sierpnia 2010 o ochronie informacji niejawnych – podstawowe wymagania
- Bezpieczeństwo fizyczne: podstawowe kryteria i sposób określania poziomu zagrożeń; dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń.
- Bezpieczeństwo fizyczne – ĆWICZENIE: metodyka doboru środków bezpieczeństwa fizycznego; klasyfikacja środków bezpieczeństwa fizycznego; Bezpieczeństwo teleinformatyczne: Systemy Zarządzania Bezpieczeństwem Informacji; Normy ISO 27001 oraz 27005; Bezpieczeństwo teleinformatyczne: Analiza ryzyka: wybór metody oraz etapy szacowania wartości informacji niejawnych i prawnie chronionych przetwarzanych w jednostce organizacyjnej.
- Bezpieczeństwo teleinformatyczne – ĆWICZENIE: identyfikacja i szacowanie zasobów informacyjnych, identyfikacja zagrożeń i określenia ich poziomu, identyfikacja podatności na ryzyka.
- Bezpieczeństwo teleinformatyczne – ĆWICZENIE: analiza i ocena ryzyka, dobór środków ochrony, akceptacja ryzyka szczytkowego; utrzymanie złożonego poziomu bezpieczeństwa informacji, przegląd ryzyk i ocena skuteczności wprowadzonego poziomu zabezpieczeń.

Harmonogram

Liczba pozycji harmonogramu: 5

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 Prawne aspekty ochrony informacji w systemach teleinformatycznych. Ogólne zasady organizacji systemu TI.	Marek Anzel	22-06-2026	08:30	12:00	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 5 bezpieczeństwo osobowe; Bezpieczeństwo fizyczne; Bezpieczeństwo elektromagnetyczne; Bezpieczeństwo kryptograficzne; Kontrola dostępu.	Marek Anzel	22-06-2026	12:00	15:00	03:00
3 z 5 Bezpieczeństwo teleinformatyczne	Marek Anzel	23-06-2026	08:30	15:00	06:30
4 z 5 Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle ustawy z dnia 5 sierpnia 2010 o ochronie informacji niejawnych – podstawowe wymagania. Bezpieczeństwo fizyczne	Marek Anzel	24-06-2026	08:30	12:00	03:30
5 z 5 Bezpieczeństwo teleinformatyczne – ĆWICZENIA	Marek Anzel	24-06-2026	12:00	15:00	03:00

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 337,00 PLN
Koszt przypadający na 1 uczestnika netto	1 900,00 PLN

Koszt osobogodziny brutto

116,85 PLN

Koszt osobogodziny netto

95,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Marek Anzel

Marek Anzel – Specjalista do spraw ochrony informacji niejawnych i systemów teleinformatycznych. Wykładowca i konsultant cyklicznych szkoleń pracowników pionów ochrony informacji niejawnych, w tym organizowanych przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Wykładowca przedmiotów z zakresu ochrony informacji niejawnych oraz działalności kancelarii tajnych na studiach podyplomowych na Uniwersytecie Śląskim i w WSB w Dąbrowie Górniczej. Autor „Vademecum kancelarii tajnej”, „Poradnika dla personelu kancelarii tajnej”, „Szacowanie Ryzyka oraz zarządzanie Ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych”, „Poradnik Specjalisty Ochrony Informacji Niejawnych”, a także wielu artykułów w prasie branżowej.

Warsztaty dla administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego.

Szacowanie i zarządzanie ryzykiem – proces analizy i oceny ryzyka

9-11 marca 2020 r. Zakopane

18-20 maja 2020 r. Sopot

24-26 czerwca 2020 r. Bukowina Tatrzańska

<https://www.ksoin.pl/szkolenia/bezpieczenstwo-teleinformatyczne/inspektor-bezpieczenstwa-teleinformatycznego-zarzadzanie-ryzykiem-warsztaty/>

wyższe

Od 2004 roku

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe uczestnicy otrzymują na podanego maila, wersja papierowa na miejscu szkolenia.

Warunki uczestnictwa

Zgłoszenie uczestnictwa i zapłata za szkolenie

Terminy:

27-29 kwietnia 2026 r. online

18-20 maja 2026 r. Rynia k. Warszawy, szkolenie stacjonarne

22-24 czerwca 2026 r. online

12-14 października 2026 r. online

7-9 grudnia 2026 r. online

Filmowy skrót naszej działalności w 2025 roku i nasze zamierzenia w 2026 roku.

<https://www.ksoin.pl/szkolenia/bezpieczenstwo-teleinformatyczne/inspektor-bezpieczenstwa-teleinformatycznego-zaradzanie-ryzykiem-warsztaty/>

Informacje dodatkowe

www.ksoin.pl

<https://www.ksoin.pl/szkolenia/bezpieczenstwo-teleinformatyczne/inspektor-bezpieczenstwa-teleinformatycznego-zaradzanie-ryzykiem-warsztaty/>

Każdy z uczestników otrzymuje materiały szkoleniowe.

Warunki techniczne

Zdalne szkolenie prowadzone przez TEAMS.

Kontakt



Biuro KSOIN

E-mail biuro@ksoin.pl

Telefon (+48) 32 2064 600