



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 2025/02/19/8548/2570595

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 20 h

📅 09.06.2025 do 11.06.2025

2 091,00 PLN brutto
1 700,00 PLN netto
104,55 PLN brutto/h
85,00 PLN netto/h

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

03-06-2025

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.	Debata swobodna

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Każdy uczestnik otrzymuje certyfikat potwierdzający zaliczenie zajęć z wynikiem pozytywnym.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Nie

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

nie

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 zarządzanie 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 szczątkowego; utrzymanie złożonego poziomu bezpieczeństwa informacji, przegląd ryzyk i ocena skuteczności wprowadzonego poziomu zabezpieczeń.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 091,00 PLN
Koszt przypadający na 1 uczestnika netto	1 700,00 PLN
Koszt osobogodziny brutto	104,55 PLN
Koszt osobogodziny netto	85,00 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.

Warunki uczestnictwa

Zgłoszenie uczestnictwa i zapłata za szkolenie

Terminy:

2-4 kwietnia 2025 r. online

23-25 kwietnia 2025 r. Krynica Morska, szkolenie stacjonarne

9-11 czerwca 2025 r. online

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

Informacje dodatkowe

www.ksoin.pl

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

Każdy z uczestników otrzymuje materiały szkoleniowe.

Warunki techniczne

Szkolenie prowadzone przez Teams.

Kontakt



Biuro KSOIN

E-mail biuro@ksoin.pl

Telefon (+48) 32 2064 600