



ŁĘTOWSKI
CONSULTING

Szkolenia,
Doradztwo, Rozwój
Mateusz Łętowski

★★★★★ 4,8 / 5

1 317 ocen

Szkolenie: Cyberbezpieczeństwo wraz z elementami Green IT.

Numer usługi 2025/11/17/12176/3152532

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 20 h

📅 30.01.2026 do 01.02.2026

5 000,00 PLN brutto

5 000,00 PLN netto

250,00 PLN brutto/h

250,00 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Grupą docelową usługi są specjaliści z sektora IT oraz menedżerowie odpowiedzialni za bezpieczeństwo informacji i zrównoważony rozwój w organizacjach. Program skierowany jest również do pracowników administracji publicznej oraz przedsiębiorstw, którzy chcą podnieść swoje kompetencje w zakresie cyberbezpieczeństwa i Green IT. Szkolenie dedykowane jest osobom dążącym do wdrażania nowoczesnych i ekologicznych rozwiązań w środowisku cyfrowym.

Minimalna liczba uczestników

3

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

23-01-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

20

Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa prowadzi do zdobycia wiedzy i praktycznych umiejętności w zakresie cyberbezpieczeństwa oraz Green IT, umożliwiających identyfikację i minimalizację zagrożeń cyfrowych, a także wdrażanie zrównoważonych technologii w organizacjach. Uczestnicy nauczą się stosować nowoczesne narzędzia i strategie wspierające ochronę danych oraz optymalizację zużycia zasobów IT. Szkolenie pozwala na rozwój kompetencji przydatnych zarówno w sektorze prywatnym, jak i publicznym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje podstawowe zasady i znaczenia cyberbezpieczeństwa oraz Green IT.	Uczestnik wyjaśnia kluczowe pojęcia, wymienia rodzaje zagrożeń i korzyści z wdrożenia Green IT.	Test teoretyczny
Uczestnik identyfikuje i ocenia zagrożenia cyfrowe w organizacji.	Uczestnik analizuje scenariusz ataku i wskazuje odpowiednie środki zapobiegawcze.	Obserwacja w warunkach symulowanych
Uczestnik stosuje narzędzia i metody wspierające cyberbezpieczeństwo.	Uczestnik skutecznie konfiguruje system dwuskładnikowego uwierzytelniania i opisuje proces szyfrowania danych.	Obserwacja w warunkach symulowanych
Uczestnik tworzy plan strategii zasad Green IT w organizacji.	Uczestnik przedstawia plan wdrożenia strategii Green IT w konkretnym środowisku pracy, uwzględniając zarządzanie energią.	Test teoretyczny
Uczestnik tworzy politykę bezpieczeństwa i zrównoważonego rozwoju.	Uczestnik opracowuje dokument polityki bezpieczeństwa lub Green IT zgodnie z wytycznymi.	Test teoretyczny
Uczestnik analizuje przypadki realnych incydentów cyberbezpieczeństwa i Green IT.	Uczestnik omawia przyczyny i skutki incydentów oraz proponuje środki zaradcze.	Obserwacja w warunkach symulowanych
Uczestnik optymalizuje zużycie energii w środowisku IT.	Uczestnik identyfikuje obszary nadmiernego zużycia energii i sugeruje odpowiednie rozwiązania techniczne.	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	Łętowski Consulting Szkolenia, Doradztwo, Rozwój Mateusz Łętowski
Podmiot prowadzący walidację jest zarejestrowany w BUR	Tak
Nazwa Podmiotu certyfikującego	SCIENCE SZKOLENIA I DORADZTWO Grzegorz Kawa
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Program

Moduł 1: Wprowadzenie do Cyberbezpieczeństwa

- 1. Definicja i znaczenie cyberbezpieczeństwa
 - Co to jest cyberbezpieczeństwo?
 - Dlaczego jest ważne?
- 2. Rodzaje zagrożeń cyberbezpieczeństwa
 - Wirusy, malware, ransomware
 - Ataki phishingowe, DDoS, man-in-the-middle
- 3. Podstawowe zasady bezpieczeństwa
 - Silne hasła i ich zarządzanie
 - Dwuskładnikowe uwierzytelnianie
 - Aktualizacje oprogramowania i systemów
- 4. Praktyczne przykłady i case studies
 - Analiza rzeczywistych incydentów

Moduł 2: Wprowadzenie do Green IT

- 1. Definicja i znaczenie Green IT
 - Co to jest Green IT?
 - Jakie są korzyści dla środowiska i organizacji?
- 2. Zrównoważone praktyki w IT
 - Eko-projektowanie sprzętu komputerowego
 - Zarządzanie energią w centrach danych
- 3. Zielone technologie i inicjatywy
 - Wirtualizacja i chmura obliczeniowa
 - Recykling i odpowiedzialne utylizowanie sprzętu
- 4. Praktyczne przykłady i case studies
 - Przykłady firm stosujących Green IT

Moduł 3: Zaawansowane Cyberbezpieczeństwo

- 1. Bezpieczeństwo sieci
 - Firewalle i systemy wykrywania intruzów (IDS/IPS)
 - VPN i zabezpieczenia sieci bezprzewodowych
- 2. Bezpieczeństwo aplikacji i danych

- Testy penetracyjne i audyty bezpieczeństwa
- Szyfrowanie danych i zarządzanie kluczami
- Zabezpieczanie gromadzonych danych
- Przesyłanie danych i informacji w sieciach publicznych

3. Zarządzanie incydentami i reakcja na incydenty

- Planowanie i procedury odpowiedzi na incydenty
- Analiza zagrożeń i informatyka śledcza

4. Prawo i regulacje dotyczące cyberbezpieczeństwa

- RODO, HIPAA, NIS2, DORA i inne regulacje

Moduł 4: Implementacja Green IT w organizacji

1. Strategie wdrażania Green IT

- Analiza i planowanie wdrożeń Green IT
- Edukacja pracowników i zmiana kultury organizacyjnej

2. Monitorowanie i optymalizacja zużycia energii

- Narzędzia do monitorowania zużycia energii
- Optymalizacja pracy serwerów i sprzętu IT

3. Zarządzanie cyklem życia sprzętu IT

- Eko-projektowanie, zakup i recykling sprzętu
- Współpraca z dostawcami ekologicznymi

4. Certyfikacje i standardy Green IT

- ISO 14001, Energy Star, i inne standardy

Moduł 5: Cyberbezpieczeństwo i Green IT w Praktyce

1. Omówienie scenariuszy ataków i obrony

- Przykłady realnych ataków hakerskich
- Praktyczne techniki obrony przed atakami

2. Warsztaty optymalizacji energii

- Praktyczne warsztaty z optymalizacji zużycia energii w organizacji
- Narzędzia do monitorowania i zarządzania energią

3. Opracowanie polityki Green IT

- Praca w grupach nad stworzeniem polityki Green IT dla organizacji
- Prezentacja i omówienie wyników prac

4. Podsumowanie i refleksja

- Dyskusja na temat zdobytej wiedzy i praktyk
- Planowanie dalszych działań w zakresie cyberbezpieczeństwa i Green IT

Egzamin.

Walidacja odbywa się w ostatnim dniu szkolenia tj. 01.02.2026 r. godzina 15:00-17:00. Egzamin prowadzony przez wyznaczoną osobę do walidacji. Certyfikacja przez jednostkę uprawnioną do certyfikacji tj. SCIENCE SZKOLENIA I DORADZTWO Grzegorz Kawa

Szkolenie prowadzone w godzinach zegarowych, w formie zajęć teoretyczno-praktycznych, tzn. Szkolenie w formie zajęć teoretyczno-praktycznych łączy przekazywanie wiedzy teoretycznej z praktycznym jej zastosowaniem.

Uczestnicy zdobywają informacje poprzez wykłady i prezentacje, a następnie wykorzystują je w praktyce podczas warsztatów i ćwiczeń w ramach każdego modułu szkolenia, gdzie ten zapis został zastosowany.

ROZDZIELNOŚĆ OSOBOWA WALIDACJI: Rozdzielność szkolenia od walidacji - rozdzielność osobowa. Osoba szkoląca nie ocenia wiedzy i umiejętności swoich kursantów w zakresie, w którym nauczała. Kończącą walidację prowadzi odrębna osoba.

Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.

Podczas szkolenia przeprowadzone zostaną pre-testy oraz post-testy wiedzy, egzamin końcowy.

Egzamin po szkoleniu potwierdza zdobycie kwalifikacji.

Nazwa kwalifikacji: **Cyberbezpieczeństwo wraz z elementami Green IT**

W ramach szkolenia jest 20 godzin zegarowych, na co składa się:

- 10 godzin zajęć teoretycznych
- 6 godzin 15 min. zajęć praktycznych
- 7 przerw po 15 min - 1 godz. 45 min
- 2 godz. walidacji

Program spełnia zakres technologii PRT z obszaru technologii informacyjnych i telekomunikacyjnych oraz technologii ochrony środowiska, w tym m.in.:

- 4.2 Technologie informacyjne
 - 4.2.4 Technologie wytwarzania oprogramowania
 - 4.2.5 Technologie data mining
- 4.6 Bezpieczeństwo informacji
 - 4.6.1 Technologie ochrony prywatności danych
- 4.7 Technologie telekomunikacyjne i informacyjne wspierające przemysł 4.0
 - 4.7.2 Technologie wspierające internet rzeczy (IoT)
 - 4.7.10 Technologie sztucznej inteligencji i uczenia maszynowego

Harmonogram

Liczba przedmiotów/zajęć: 17

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 17 Moduł 1: Wprowadzenie do Cyberbezpieczeństwa. Zajęcia teoretyczno-praktyczne.	Adam Parysz	30-01-2026	17:00	18:45	01:45
2 z 17 Przerwa.	Adam Parysz	30-01-2026	18:45	19:00	00:15
3 z 17 Moduł 1: Wprowadzenie do Cyberbezpieczeństwa. Zajęcia teoretyczno-praktyczne.	Adam Parysz	30-01-2026	19:00	21:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 17 Moduł 2: Wprowadzenie do Green IT. Zajęcia teoretyczno-praktyczne.	Adam Parysz	31-01-2026	09:00	10:45	01:45
5 z 17 Przerwa.	Adam Parysz	31-01-2026	10:45	11:00	00:15
6 z 17 Moduł 2: Wprowadzenie do Green IT. Zajęcia teoretyczno-praktyczne.	Adam Parysz	31-01-2026	11:00	12:45	01:45
7 z 17 Przerwa.	Adam Parysz	31-01-2026	12:45	13:00	00:15
8 z 17 Moduł 3: Zaawansowane Cyberbezpieczeństwo. Zajęcia teoretyczno-praktyczne.	Adam Parysz	31-01-2026	13:00	14:45	01:45
9 z 17 Przerwa.	Adam Parysz	31-01-2026	14:45	15:00	00:15
10 z 17 Moduł 3: Zaawansowane Cyberbezpieczeństwo. Zajęcia teoretyczno-praktyczne.	Adam Parysz	31-01-2026	15:00	17:00	02:00
11 z 17 Moduł 4: Implementacja Green IT w organizacji. Zajęcia teoretyczno-praktyczne.	Adam Parysz	01-02-2026	09:00	10:45	01:45
12 z 17 Przerwa.	Adam Parysz	01-02-2026	10:45	11:00	00:15
13 z 17 Moduł 4: Implementacja Green IT w organizacji. Zajęcia teoretyczno-praktyczne.	Adam Parysz	01-02-2026	11:00	12:45	01:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 17 Przerwa.	Adam Parysz	01-02-2026	12:45	13:00	00:15
15 z 17 Moduł 5: Cyberbezpieczeństwo i Green IT w Praktyce. Zajęcia teoretyczno-praktyczne.	Adam Parysz	01-02-2026	13:00	14:45	01:45
16 z 17 Przerwa.	Adam Parysz	01-02-2026	14:45	15:00	00:15
17 z 17 Walidacja.	-	01-02-2026	15:00	17:00	02:00

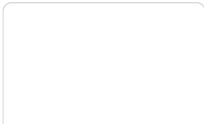
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	250,00 PLN
W tym koszt walidacji brutto	100,00 PLN
W tym koszt walidacji netto	100,00 PLN
W tym koszt certyfikowania brutto	250,00 PLN
W tym koszt certyfikowania netto	250,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1
Adam Parysz



Od 2013 roku Adam Parysz jest cenionym trenerem i szkoleniowcem. Spędził ponad 13 521 godzin na prowadzeniu szkoleń, podczas których przeszkolił ponad 15 tysięcy uczestników. Auditor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg. normy PN-EN ISO/IEC 27001, Auditor Wiodący Systemu Zarządzania Ciągłością Działania wg. normy ISO 22301, Auditor wewnętrzny zintegrowanego systemu zarządzania wg ISO 9001, ISO 14001 oraz ISO 45001, Auditor Wewnętrzny standardu TISAX, Certyfikowany SIX SIGMA YELLOW BELT, Archiwista, Wdrożeniowiec systemów klasy ESD, Inspektor Ochrony Danych Osobowych, Specjalista ds. AI. Członek Zwyczajny ISSA Polska (Grupa Robocza ds. AI), Członek Grupy Roboczej ds. Sztucznej Inteligencji przy Ministerstwie Cyfryzacji, Autor książki "Polecenia dla ChatGPT w finansach", Autor artykułów dla Legalis Administracja wydawnictwa C.H. Beck, uczestnik programów CampusAI oraz Umiejętności Jutra Google. Biegła znajomość narzędzi AI: ChatGPT, Microsoft Copilot, Google Gemini, Adobe Firefly i Midjourney. Orientacja na działanie oraz skuteczne zarządzanie czasem pracy. Umiejętność zarządzania konfliktem i radzenia sobie ze stresem. Komunikatywność. Od 5 lat prowadzenie szkoleń, warsztatów, wykładów z zakresu Sztucznej Inteligencji oraz wykorzystania jej potencjału w różnych dziedzinach w tym w rozwoju firmy, sprzedaży, obsługi z uwzględnieniem zrównoważonego rozwoju i optymalizacji rozwoju przedsiębiorstw.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Opracowania własne trenera, prezentacja, skrypty szkoleniowe.

Informacje dodatkowe

Dla uczestników z dofinansowaniem min. 70% kwoty szkolenia - stawka „zw” – „§ 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

Warunki techniczne

iOS: iOS 11

Windows: Windows 10 kompilacja 14393

Android: Android OS 5.0

Funkcje sieci Web. Najnowsza wersja przeglądarki Safari, Internet Explorer 11, Chrome, Edge lub Firefox

Komputer Mac: MacOS 10.13

Połączenie internetowe: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach:

- dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie).

- dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie).

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Kontakt

Justyna Hebda



E-mail justynahebda@letowskiconsulting.pl

Telefon (+48) 518 178 151