Możliwość dofinansowania

Cyberbezpieczeństwo: Ochrona danych i systemów informatycznych

Numer usługi 2025/09/21/8973/3022006

4 000,00 PLN brutto
4 000,00 PLN netto
133,33 PLN brutto/h
133,33 PLN netto/h

"Akademia Zdrowia"
Izabela Łajs

4,7 / 5
69 ocen

Kielce / stacjonarna
Usługa szkoleniowa
30 h
17.11.2025 do 20.11.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do: • Pracownicy działów IT i informatycy odpowiedzialni za bezpieczeństwo systemów informatycznych. • Specjaliści ds. bezpieczeństwa informacji i cyberbezpieczeństwa. • Kierownictwo i kadra zarządzająca, odpowiedzialna za podejmowanie decyzji dotyczących bezpieczeństwa cybernetycznego. • Specjaliści zainteresowani rozwojem zawodowym w dziedzinie cyberbezpieczeństwa. • Wszystkie osoby zainteresowane omawianą podczas szkolenia tematyką.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	10-11-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	30
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

Przygotowanie uczestników do umiejętności efektywnego wykorzystywania Chat GPT i innych urządzeń AI w pracy, edukacji oraz w codziennych obowiązkach, by sprostać rosnącemu zapotrzebowaniu na wiedzę w tej dziedzinie oraz wpłynąć na rozwój swojej kariery.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe zagrożenia cyfrowe	definiuje aktualne zagrożenia w Polsce i na świecie	Test teoretyczny
	rozpoznaje i klasyfikuje przykłady ataków phishingowych, ransomware iinnych zagrożeń	Test teoretyczny
Planuje zasady bezpiecznej pracy zdanymi i urządzeniami	Definiuje podstawy prawne i standardy bezpieczeństwa w firmie	Test teoretyczny
	Opracowuje zasady zarządzania nośnikami danych	Test teoretyczny
Rozróżnia bezpieczne i niebezpieczne praktyki w zakresie zarządzania hasłami i kontami.	Opracowuje uwierzytelniające hasła oraz wskazuje elementy wymagające poprawy w zabezpieczeniu haseł	Test teoretyczny
Opracowuje metody pracy zgodne z podstawowymi zasadami bezpieczeństwa systemów i urządzeń	Stosuje ustawienia zabezpieczeń i aktualizacji	Test teoretyczny
Stosuje metody bezpiecznej komunikacji online oraz ochrony tożsamości cyfrowej	Stosuje odpowiednie działania w przypadku podejrzenia phishingu, fałszywych źródeł lub naruszenia prywatności.	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	uprawnionych do wydawania dokumentów potwierdzających uzyskanie kwalifikacji, w tym w zawodzie

Nazwa Podmiotu prowadzącego walidację	Certyfikacja ICVC Sp z o.o.
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa Podmiotu certyfikującego	Certyfikacja ICVC Sp z o.o.
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

Zajęcia teoretyczne:

- Historia cyberzagrożeń i ewolucja ataków.
- Kluczowe pojęcia: zagrożenie, podatność, incydent bezpieczeństwa.
- Przegląd najczęstszych rodzajów zagrożeń.
- Phishing: typy, techniki wykrywania i zapobiegania.
- Malware: rodzaje (wirusy, trojany, ransomware, spyware).
- Ataki DDoS: typy, mechanizmy działania.
- Metody analizy i klasyfikacji zagrożeń, narzędzia wykrywania: IDS/IPS, SIEM.
- Przegląd narzędzi i analiza przykładowych incydentów.
- Szyfrowanie symetryczne i asymetryczne, haszowanie, podpis cyfrowy.
- Przegląd algorytmów (AES, RSA, SHA-256).
- Struktura i zastosowanie SSL/TLS, certyfikaty cyfrowe.
- Przegląd najbardziej powszechnych protokołów komunikacyjnych: SSH, PGP, HTTPS, WPA
- Przegląd typów VPN (SSL VPN, IPSec VPN), konfiguracja połączenia VPN
- Proces analizy ryzyka w cyberbezpieczeństwie.
- Techniki identyfikacji ryzyka.
- Przegląd strategii zarządzania ryzykiem.
- Opracowanie strategii zarządzania ryzykiem dla wybranego scenariusza.
- Elementy strategii bezpieczeństwa i zarządzanie ryzykiem.
- Tworzenie planu zarządzania ryzykiem.
- Proces testów penetracyjnych i narzędzia.
- Symulacja testu penetracyjnego i tworzenie raportu.
- Zasady i narzędzia audytu bezpieczeństwa.
- Wykonanie przykładowego audytu bezpieczeństwa
- Techniki oceny podatności, narzędzia skanowania.
- Przegląd regulacji międzynarodowych i krajowych.
- Dyskusja na temat wdrażania regulacji.
- Kluczowe zasady RODO, przetwarzanie danych zgodnie z RODO
- Zasady etyczne oraz odpowiedzialność prawna.
- Analiza przypadków naruszeń etyki i prawa.

Zajęcia praktyczne:

- Ćwiczenia w identyfikacji najczęściej spotykanych metod ataku w sieci.
- Ćwiczenia: szyfrowanie i deszyfrowanie danych.
- Ćwiczenia: analiza ryzyka dla przykładowego środowiska IT.
- Ćwiczenia: przeprowadzenie oceny podatności

Każdy z kursantów ma do dyspozycji stanowisko pracy i komputer.

Usługa w swojej cenie zawiera koszty walidacji.

Usługa jest prowadzona w trybie godzin dydaktycznych. 30 godzin dydaktycznych = 22 godziny zegarowe i 30min .

Przerwy nie wliczają się w czas trwania usługi. W ciągu dnia przewidziana jest przerwa 30 minut .

Harmonogram

Liczba przedmiotów/zajęć: 14

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Historia cyberzagrożeń i ewolucja ataków. Kluczowe pojęcia: zagrożenie, podatność, incydent bezpieczeństwa. Przegląd najczęstszych rodzajów zagrożeń.	mgr inż. Przemysław Kaczmarski	17-11-2025	09:00	12:00	03:00
2 z 14 Przerwa	mgr inż. Przemysław Kaczmarski	17-11-2025	12:00	12:30	00:30
3 z 14 Malware: rodzaje (wirusy, trojany, ransomware, spyware). Ataki DDoS: typy, mechanizmy działania. Metody analizy i klasyfikacji zagrożeń, narzędzia wykrywania: IDS/IPS, SIEM.	mgr inż. Przemysław Kaczmarski	17-11-2025	12:30	14:30	02:00
4 z 14 Przegląd narzędzi i analiza przykładowych incydentów. Szyfrowanie symetryczne i asymetryczne, haszowanie, podpis cyfrowy. Przegląd algorytmów (AES, RSA, SHA-256).	mgr inż. Przemysław Kaczmarski	18-11-2025	08:30	12:00	03:30
5 z 14 Przerwa	mgr inż. Przemysław Kaczmarski	18-11-2025	12:00	12:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 14 Struktura i zastosowanie SSL/TLS, certyfikaty cyfrowe. Przegląd najbardziej powszechnych protokołów komunikacyjnych : SSH, PGP, HTTPS, WPA Przegląd typów VPN (SSL VPN, IPSec VPN),	mgr inż. Przemysław Kaczmarski	18-11-2025	12:30	14:30	02:00
7 z 14 Proces analizy ryzyka w cyberbezpieczeń stwie. Techniki identyfikacji ryzyka. Przegląd strategii zarządzania ryzykiem. Opracowanie strategii zarządzania ryzykiem dla wybranego scenariusza.	mgr inż. Przemysław Kaczmarski	19-11-2025	08:30	12:00	03:30
8 z 14 Przerwa	mgr inż. Przemysław Kaczmarski	19-11-2025	12:00	12:30	00:30
9 z 14 Elementy strategii bezpieczeństwa i zarządzanie ryzykiem. Tworzenie planu zarządzania ryzykiem. Proces testów penetracyjnych i narzędzia. Symulacja testu penetracyjnego i tworzenie raportu.	mgr inż. Przemysław Kaczmarski	19-11-2025	12:30	14:30	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 14 Zasady i narzędzia audytu bezpieczeństwa. Wykonanie przykładowego audytu bezpieczeństwa Techniki oceny podatności, narzędzia skanowania. Przegląd regulacji międzynarodowych i krajowych.	mgr inż. Przemysław Kaczmarski	20-11-2025	08:30	11:00	02:30
11 z 14 Dyskusja na temat wdrażania regulacji. Kluczowe zasady RODO, przetwarzanie danych zgodnie z RODO Zasady etyczne oraz odpowiedzialność prawna. Analiza przypadków naruszeń etyki i prawa.	mgr inż. Przemysław Kaczmarski	20-11-2025	11:00	12:00	01:00
12 z 14 Przerwa	mgr inż. Przemysław Kaczmarski	20-11-2025	12:00	12:30	00:30
13 z 14 Ćwiczenia w identyfikacji najczęściej spotykanych metod ataku w sieci. Szyfrowanie i deszyfrowanie danych. Analiza ryzyka dla przykładowego środowiska IT. Ćwiczenia: przeprowadzenie oceny podatności	mgr inż. Przemysław Kaczmarski	20-11-2025	12:30	15:00	02:30
14 z 14 Egzamin ICVC	-	20-11-2025	15:00	15:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 000,00 PLN
Koszt przypadający na 1 uczestnika netto	4 000,00 PLN
Koszt osobogodziny brutto	133,33 PLN
Koszt osobogodziny netto	133,33 PLN
W tym koszt walidacji brutto	170,00 PLN
W tym koszt walidacji netto	170,00 PLN
W tym koszt certyfikowania brutto	30,00 PLN
W tym koszt certyfikowania netto	30,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

mgr inż. Przemysław Kaczmarski

Specjalista IT, wykładowca akademicki oraz trener z wieloletnim doświadczeniem w branży informatycznej. Absolwent Wyższej Szkoły Handlowej w Kielcach na kierunku Ekonomia ze specjalnością ekonomiczne zastosowania informatyki oraz Zarządzanie i Marketing. Ukończył również studia podyplomowe z zakresu matemtyki, administracji sieci komputerowych oraz cyberbezpieczeństwa. Posiada liczne certyfikaty m.in. Cisco Academy (Introduction to Cybersecurity), Microsoft oraz certyfikat Egzaminatora DIGITAL EUROPE.
Na co dzień zajmuje się tworzeniem stron internetowych, administracją i systemami IT oraz prowadzi zajęcia z programowania. Od 2025 wykładowca na kierunku Informatyka w Uniwersytecie WSB Merito w Poznaniu. Prowadzi również liczne szkolenia z zakresu cyberbezpieczeństwa w ramach projektów edukacyjnych

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypt szkoleniowy.

Informacje dodatkowe

1 godzina = 45 minut

Zwolniony z VAT na podstawie ustawa VAT art. 43 ust. 1 pkt 26a

Usługa w swojej cenie zawiera koszty walidacji.

Adres

al. IX Wieków Kielc 8/24
25-516 Kielce
woj. świętokrzyskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Agnieszka Zięba

E-mail agnieszka.zieba@akademia-zdrowia.pl
Telefon (+48) 662 536 086