



PROFITONIC Maciej
Leonard

★★★★★ 4,8 / 5

749 ocen

CYBER SAFE – cyberbezpieczeństwo i zielona transformacja cyfrowa. Kwalifikacje. Szkolenie.

Numer usługi 2026/08/14/119739/3747214

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 16:00 h
- 📅 14.09.2026 do 16.09.2026

5 535,00 PLN brutto

4 500,00 PLN netto

345,94 PLN brutto/h

281,25 PLN netto/h

233,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Internet

Grupa docelowa usługi

Szkolenie skierowane jest do osób, które planują z własnej inicjatywy podnieść swoje umiejętności w zakresie **kwalifikacji cyfrowych i cyberbezpieczeństwa**, w szczególności bezpiecznego korzystania z komputera, Internetu, poczty elektronicznej, usług chmurowych oraz nowoczesnych technologii.

Usługa prowadzi do zdobycia kwalifikacji międzynarodowej: **GCCS/ICVC Specjalista ds. cyberbezpieczeństwa (ICVC/CBB 207771.19)**.

Usługa skierowana jest również do osób chcących rozwijać **zielone kompetencje** w zakresie bezpiecznego i zrównoważonego wykorzystywania technologii cyfrowych, w tym świadomego zarządzania danymi, ograniczania ich nadmiaru, energooszczędnego korzystania ze sprzętu i usług cyfrowych oraz odpowiedzialnej ochrony informacji i prywatności

Minimalna liczba uczestników

3

Maksymalna liczba uczestników

16

Data zakończenia rekrutacji

13-09-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

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

Celem usługi jest nabycie przez uczestnika wiedzy i umiejętności umożliwiających bezpieczne korzystanie z technologii cyfrowych oraz skuteczne reagowanie na podstawowe cyberzagrożenia. Uczestnik nauczy się chronić dane, konta i prywatność, rozpoznawać próby oszustw i zagrożenia w sieci oraz świadomie korzystać z Internetu, poczty, chmury i AI. Rozwinie również zielone kompetencje związane z eko-IT, ograniczaniem śladu cyfrowego i odpowiedzialnym wykorzystaniem technologii.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe zasady cyberbezpieczeństwa	Rozróżnia podstawowe rodzaje zagrożeń cyfrowych.	Test teoretyczny
	Wskazuje zasady bezpiecznego korzystania z urządzeń, systemów i Internetu	Test teoretyczny
Rozpoznaje zagrożenia występujące w środowisku cyfrowym	Rozróżnia phishing, smishing, vishing, złośliwe oprogramowanie i socjotechnikę	Test teoretyczny
	Identyfikuje cechy podejrzanych wiadomości, linków i stron internetowych.	Test teoretyczny
	Dobiera zabezpieczenia odpowiednio do rodzaju zagrożenia	Test teoretyczny
Dobiera właściwe sposoby zabezpieczania danych i urządzeń	Wskazuje właściwe działania dotyczące haseł, aktualizacji, kopii zapasowych i uwierzytelniania wieloskładnikowego.	Test teoretyczny
	Dobiera właściwe sposoby przechowywania, udostępniania i archiwizacji danych	Test teoretyczny
	Rozróżnia działania zwiększające i obniżające bezpieczeństwo informacji.	Test teoretyczny
Stosuje zasady bezpiecznego i odpowiedzialnego zarządzania informacją	Rozpoznaje sytuacje wymagające reakcji na incydent bezpieczeństwa i wskazuje właściwy sposób postępowania.	Test teoretyczny
	Uwzględnia odpowiedzialność użytkownika za bezpieczeństwo danych i informacji.	Test teoretyczny
Jest gotowy do odpowiedzialnego reagowania na zagrożenia cyfrowe	Rozpoznaje sytuacje wymagające reakcji na incydent bezpieczeństwa i wskazuje właściwy sposób postępowania.	Test teoretyczny
	Uwzględnia odpowiedzialność użytkownika za bezpieczeństwo danych i informacji.	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://standardgccs.com/>

Strona internetowa Instytucji Walidującej: <https://icvc.eu/>

Informacje

Nazwa Podmiotu prowadzącego walidację	ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Nazwa Podmiotu certyfikującego	TALENT ODYSSEY LTD.

Program

Informacje dotyczące realizacji usługi, walidacji i certyfikacji

Usługa realizowana jest w wymiarze **16 godzin zegarowych**, przy czym 1 godzina odpowiada 60 minutom. Program obejmuje zajęcia teoretyczne, praktyczne oraz walidację efektów uczenia się.

Przerwy nie są wliczane do czasu trwania usługi.

Szkolenie realizowane jest w formule zdalnej w czasie rzeczywistym. Zajęcia obejmują część teoretyczną oraz praktyczną, w tym prezentacje, demonstracje, analizę przykładów, studia przypadków oraz ćwiczenia pozwalające uczestnikom zastosować omawiane zasady cyberbezpieczeństwa w codziennej pracy i korzystaniu z technologii cyfrowych.

Program szkolenia rozwija również **zielone kompetencje**, w szczególności w zakresie odpowiedzialnego korzystania z urządzeń i usług cyfrowych, eko-IT, cyfrowego minimalizmu, racjonalnego zarządzania danymi, ograniczania zbędnego transferu i przechowywania informacji oraz wydłużania cyklu życia sprzętu.

Usługa przygotowuje uczestników do uzyskania międzynarodowej kwalifikacji:

„GCCS/ICVC Specjalista ds. cyberbezpieczeństwa (ICVC/CBB 207771.19)”.

Walidacja efektów uczenia się przeprowadzana jest przez ICVC Certyfikacja Sp. z o.o. Walidacja odbywa się w formie **testu teoretycznego** i ma na celu potwierdzenie osiągnięcia przez uczestnika efektów uczenia się oraz spełnienia przypisanych do nich kryteriów weryfikacji.

Proces walidacji jest **oddzielony od procesu kształcenia**. Osoba przeprowadzająca walidację nie uczestniczy w prowadzeniu zajęć szkoleniowych, co zapewnia rozdzielność procesu kształcenia i procesu walidacji.

Podmiotem certyfikującym jest Talent Odyssey Ltd.

Warunkiem uzyskania kwalifikacji jest osiągnięcie wymaganych efektów uczenia się oraz **pozytywne przejście procesu walidacji**. Po spełnieniu wymagań uczestnik otrzymuje certyfikat potwierdzający uzyskanie kwalifikacji.

Ramowy program usługi – 16 godzin

DZIEŃ 1 – CYBERBEZPIECZEŃSTWO W CODZIENNEJ PRACY CYFROWEJ

1. Świadomy użytkownik w cyfrowym świecie

- podstawowe pojęcia związane z cyberbezpieczeństwem,
- bezpieczeństwo urządzeń, systemów i danych,
- najczęstsze źródła zagrożeń cyfrowych,
- aktualizacje systemów i aplikacji,
- bezpieczna konfiguracja urządzeń,
- odpowiedzialność użytkownika za bezpieczeństwo cyfrowe,
- wpływ urządzeń i infrastruktury cyfrowej na środowisko.

2. Cyberzagrożenia – rozpoznawanie i reagowanie

- phishing, smishing i vishing,
- socjotechnika i manipulacja użytkownikiem,
- złośliwe oprogramowanie,
- niebezpieczne załączniki i linki,
- fałszywe strony internetowe, sklepy i formularze logowania,
- rozpoznawanie symptomów cyberataku,
- właściwe postępowanie w przypadku wykrycia zagrożenia.

3. Hasła, konta i ochrona tożsamości cyfrowej

- zasady tworzenia silnych haseł i fraz hasłowych,
- bezpieczne zarządzanie hasłami,
- menedżery haseł,
- uwierzytelnianie wieloskładnikowe MFA/2FA,
- zabezpieczanie kont prywatnych i służbowych,
- wycieki danych i sposoby reagowania,
- ochrona cyfrowej tożsamości użytkownika.

4. Bezpieczny Internet i poczta elektroniczna

- ocena wiarygodności stron internetowych,
- domeny, HTTPS i certyfikaty bezpieczeństwa,
- bezpieczne pobieranie plików,
- rozpoznawanie podejrzanych wiadomości e-mail,
- bezpieczeństwo korzystania z publicznych sieci Wi-Fi,
- bezpieczna komunikacja online,
- dobre praktyki podczas korzystania z Internetu.

5. Bezpieczeństwo danych, chmura i cyfrowy minimalizm

- zasady bezpiecznego przechowywania danych,
- kopie zapasowe i archiwizacja,
- bezpieczne udostępnianie plików,
- bezpieczeństwo usług chmurowych,
- porządkowanie danych i eliminowanie duplikatów,
- ograniczanie zbędnego przechowywania informacji,
- cyfrowy minimalizm jako element bezpieczeństwa i zrównoważonego rozwoju.

DZIEŃ 2 – AI, OCHRONA INFORMACJI I ZIELONE CYBERBEZPIECZEŃSTWO

6. Sztuczna inteligencja a cyberbezpieczeństwo

- wykorzystanie AI we współczesnym środowisku cyfrowym,

- zagrożenia związane z generatywną sztuczną inteligencją,
- phishing i oszustwa wspomagane przez AI,
- deepfake i klonowanie głosu,
- dezinformacja i treści generowane przez AI,
- zasady bezpiecznego przekazywania informacji do narzędzi AI,
- ochrona danych firmowych i osobowych podczas korzystania z AI.

7. Prywatność i odpowiedzialne zarządzanie informacją

- dane osobowe i informacje poufne,
- ochrona prywatności użytkownika,
- ustawienia prywatności w usługach cyfrowych,
- bezpieczne udostępnianie informacji,
- ograniczanie cyfrowego śladu użytkownika,
- odpowiedzialne korzystanie z aplikacji i usług online,
- dobre praktyki ochrony informacji w środowisku zawodowym.

8. ECO CYBER – zielone kompetencje w środowisku cyfrowym

- Green IT i odpowiedzialne korzystanie z technologii,
- wpływ przechowywania i przesyłania danych na środowisko,
- ograniczanie zbędnego transferu danych,
- racjonalne korzystanie z przestrzeni chmurowej,
- energooszczędne korzystanie z komputerów i urządzeń mobilnych,
- wydłużanie cyklu życia sprzętu,
- e-odpady i gospodarka obiegu zamkniętego (GOZ),
- świadome korzystanie z narzędzi AI i zasobów cyfrowych,
- ograniczanie zbędnych operacji cyfrowych i generacji AI.

9. Cyberbezpieczeństwo w praktyce – warsztat

- analiza przykładowych wiadomości phishingowych,
- rozpoznawanie podejrzanych linków i stron,
- analiza przykładowych incydentów bezpieczeństwa,
- dobór zabezpieczeń do rodzaju zagrożenia,
- ocena bezpieczeństwa kont i usług cyfrowych,
- reagowanie na incydenty,
- tworzenie własnego zestawu dobrych praktyk cyberbezpieczeństwa.

10. Bezpieczna i odpowiedzialna praca cyfrowa

- bezpieczne współdzielenie dokumentów i plików,
- komunikacja za pomocą poczty i komunikatorów,
- bezpieczeństwo pracy zdalnej,
- odpowiedzialność użytkownika za dane i informacje,
- budowanie bezpiecznych nawyków cyfrowych,
- łączenie cyberbezpieczeństwa z zasadami zrównoważonego rozwoju,
- rozwijanie kompetencji cyfrowych i zielonych.

11. Przygotowanie do walidacji i walidacja efektów uczenia się

- podsumowanie kluczowych zagadnień objętych kwalifikacją,
- uporządkowanie wiedzy przed walidacją,
- przygotowanie uczestników do procesu walidacji,
- **walidacja efektów uczenia się – test teoretyczny.**

Harmonogram

Liczba pozycji harmonogramu: 6

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 zajęcia	Zajęcia	MACIEJ LEONARD	14-09-2026	08:00	14:00	06:00
2 z 6 -	Przerwa	-	14-09-2026	14:00	15:00	01:00
3 z 6 zajęcia	Zajęcia	MACIEJ LEONARD	15-09-2026	08:00	14:15	06:15
4 z 6 -	Przerwa	-	15-09-2026	14:15	15:15	01:00
5 z 6 zajęcia	Zajęcia	MACIEJ LEONARD	16-09-2026	08:00	09:00	01:00
6 z 6 -	Walidacja	-	16-09-2026	09:00	09:45	00:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:15
w tym suma godzin walidacji	00:45
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 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 w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
-------------	------

Koszt przypadający na 1 uczestnika brutto	5 535,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	345,94 PLN
Koszt osobogodziny netto	281,25 PLN
W tym koszt walidacji brutto	209,10 PLN
W tym koszt walidacji netto	170,00 PLN
W tym koszt certyfikowania brutto	209,10 PLN
W tym koszt certyfikowania netto	170,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1



1 z 1

MACIEJ LEONARD

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Warunki techniczne

Kontakt



Karolina Czajkowska

E-mail karolina.czajkowska99@gmail.com

Telefon (+48) 514 970 108