

**[Kierunek - Rozwój] Cisco Network Security (tryb mieszany)**

Numer usługi 2026/04/12/165599/3480740

6 400,00 PLN brutto

6 400,00 PLN netto

82,05 PLN brutto/h

82,05 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Fundacja
ALTERnacja

★★★★★ 4,6 / 5

89 ocen

📍 Bydgoszcz

🏢 Usługa szkoleniowa

📄 mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

🕒 78:00 h

📅 04.09.2026 do 27.11.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Identyfikatory projektów

Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Zachodniopomorskie Bony Szkoleniowe, Małopolski Pociąg do kariery, Regionalny Fundusz Szkoleniowy II

Grupa docelowa usługi

Szkolenie przeznaczone jest dla osób fizycznych lub pracowników firm:

- pracujących w branży sieciowej, pragnących poszerzyć lub uzupełnić wiedzę za zakresu realizacji poufności informacji przesyłanych przez sieć Internet oraz przeciwdziałania cyberatakam,
- operatorskich (inżynierów sieci), który zamierzają pozyskać umiejętności związane z zabezpieczeniem infrastruktury IT firmy (CyberSEC),
- zainteresowanych wdrażaniem tuneli VPN oraz dostępu zdalnego do infrastruktury firmowej.
- chcących poszerzyć lub uporządkować wiedzę i umiejętności dotyczące zabezpieczenia sieci i urządzeń Cisco, tj. przełączników, routerów, firewalli,
- działów IT zarządzających infrastrukturę teleinformatyczną,
- pracujących na stanowiskach informatyka w MŚP, świadomych poziomu zagrożenia cyberprzestępczością,
- chcących uzupełnić wiedzę i kwalifikacje z zakresu bezpieczeństwa sieci korporacyjnych i kampusowy,
- planujących przebranżowienie wewnątrz firmy na stanowiska typu CyberSEC.

Dla uczestników proj. Kierunek - Rozwój

Minimalna liczba uczestników

8

Maksymalna liczba uczestników

17

Data zakończenia rekrutacji	03-09-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	78
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Usługa „Cisco Network Security - kurs zaawansowany” przygotowuje do podjęcia pracy i samodzielnej realizacji zadań inżyniera bezpieczeństwa sieci (CyberSec / SIEM).

Usługa „Cisco Network Security - kurs zaawansowany” przygotowuje do samodzielnej konfiguracji i weryfikacji działania następujących rozwiązań i komponentów sieciowych: VPN, IPS, ACL, Firewall, protokoły kryptograficzne, routery brzegowe.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje zagrożenia bezpieczeństwa, z którymi borykają się nowoczesne infrastruktury sieciowe.	Rozróżnia zagrożenia bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje politykę zabezpieczeń dla routerów Cisco.	Rozróżnia zagrożenie i metody przeciwdziałania atakom	Test teoretyczny z wynikiem generowanym automatycznie
Planuje wdrożenie AAA na routerach Cisco, wykorzystując lokalną bazę danych routera oraz zewnętrzny serwer.	Definiuje konfigurację AAA w urządzeniu sieciowym	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia zagrożenia dla routerów i sieci Cisco za pomocą list kontroli dostępu (ACL).	Projektuje listy kontroli dostępu.	Test teoretyczny z wynikiem generowanym automatycznie
Zarządza sieciami w sposób zapewniający bezpieczeństwo.	Uzasadnia konieczność wdrożenie odpowiednich mechanizmów bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje urządzenia sieciowe w sposób chroniący sieć przed atakami na warstwę 2.	Zabezpiecza przełączniki sieciowe przed atakiem do strony sieci LAN.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Projektuje zestawy funkcji firewalla Cisco IOS.	Definiuje działania firewalla.	Test teoretyczny z wynikiem generowanym automatycznie
Implementuje urządzenie Cisco ASA w celu świadczenia usług zapory sieciowej oraz translacji adresów sieciowych (NAT/PAT).	Wdraża i weryfikuje konfigurację firewalla sprzętowego ASA.	Test teoretyczny z wynikiem generowanym automatycznie
Planuje i wdraża tunele VPN typu site-to-site z wykorzystaniem IPsec	Definiuje parametry protokołów kryptograficznych używanych do budowy tuneli VPN.	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje parametry protokołów kryptograficznych używanych do budowy tuneli VPN.	Rozróżnia protokoły szyfrowania oraz algorytmy zapewnienia integralności.	Test teoretyczny z wynikiem generowanym automatycznie
Uzasadnia potrzebę używania firewall'i Zone-Based Policy.	Definiuje ruch interesujący przechodzący przez firewall.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

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

TAK

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

Strona internetowa Instytucji Walidującej: <https://alternacja.pl/cisco>

Informacje

Nazwa Podmiotu prowadzącego walidację	Fundacja ALTERnacja - Lokalna Akademia Cisco ID 20043915, wpisana do BUR
Nazwa Podmiotu certyfikującego	Cisco Networking Academy, której członkiem jest Fundacja ALTERnacja (Lokalna Akademia Cisco ID 20043915) - zarejestrowana w BUR

Program

Kurs Cisco Network Security jest rozpoznawalnym na świecie kursem związanym z bezpieczeństwem sieci i infrastruktury sieciowym, w skrócie CyberSEC. Zawartość merytoryczna kolejnych modułów została tak dobrana, aby uczestnik szkolenia zapoznawał się kolejno i stopniowo z protokołami oraz mechanizmami sieciowymi niwelującymi próby cyberataku z wnętrza organizacji oraz od strony Internetu.

Kurs Cisco Network Security składa się z 22 modułów:

1. Zabezpieczanie sieci
2. Zagrożenia sieciowe
3. Ograniczanie zagrożeń sieciowych
4. Bezpieczny dostęp do urządzeń
5. Role administracyjne
6. Zarządzanie i monitorowanie urządzeń
7. AAA – autoryzacja, uwierzytelnienie i rejestracja
8. ACL – listy kontroli dostępu
9. Technologie Firewall'i
10. Zone-Based Policy Firewall
11. Technologia IPS
12. Implementacja i działanie IPS
13. Zabezpieczanie urządzeń końcowych
14. Bezpieczeństwo warstwy L2 sieci
15. Usługi i protokoły kryptograficzne
16. Postawy uwierzytelnienia i integralności
17. Infrastruktura klucza publicznego
18. VPN – wirtualne sieci prywatne
19. Implementacja Site-to-Site VPN
20. Podstawowa konfiguracja ASA
21. Konfiguracja firewall'a w ASA
22. Testowanie zabezpieczeń sieci

Oficjalne materiały szkoleniowe Cisco składają się z:

- 22 modułów tematycznych
- 23 ćwiczeń wykonywanych na sprzęcie,
- 22 zadań symulacyjnych do realizacji w środowisku Packet Tracer
- 87 ćwiczeń interaktywnych w tym materiały video i quizy,
- 8 egzaminów modułowych
- 1 egzamin końcowy uprawniający do otrzymania certyfikatu ukończenia szkolenia wraz ze zdobytymi kompetencjami.

Sposób prowadzenia szkolenia:

- Kurs prowadzony jest przez certyfikowanego trenera Cisco w języku polskim, wykłady prowadzone są po polsku.
- Student otrzymuje dostęp do certyfikowanych materiałów szkoleniowych oraz egzaminów i ćwiczeń laboratoryjnych w języku angielskim.
- Ćwiczenia rozszerzające oficjalne treści, przygotowane zostały w języku polskim.
- zajęcia praktyczne realizowane są w zespołach 2-3 osobowych. Każdy student Akademii Cisco ma dostęp do indywidualnego komputera PC, przełącznika Cisco 2960, routera Cisco 4021, routera Cisco 2801 oraz firewalla ASA.

Forma kursu:

- Szkolenie trwać będzie 78 godzin lekcyjnych, z czego 66 godzin będzie realizowanych zdalnie w czasie rzeczywistym, 12 godzin lekcyjnych z laboratorium sieciowym. Zajęcia ze sprzętem sieciowym będą realizowane w laboratorium sieciowym Wydziału Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. W trakcie zajęć każdy uczestnik będzie miał dostęp do fizycznego sprzętu Cisco i indywidualnego komputera, co pozwoli realizować zadania przewidziane w kursie Cisco oraz zadania dodatkowe przygotowane przez trenerów. Uczestnicy będą mieli dostęp do 30 routerów Cisco, 18 przełączników Catalyst i 10 firewalli Cisco ASA.

Charakterystyka kursu:

<https://alternacja.pl/cisco/wp-content/uploads/2023/11/Network-Security-v1.0-Product-Overview.pdf>

Warunki organizacyjne dla przeprowadzenia szkolenia:

- w trakcie zajęć praktycznych uczestnicy szkolenia będą realizowali konfiguracyjne zadania praktyczne w zespołach 2 lub 3 osobowych, zależnie od konkretnego zadania. Każdy zespół będzie konfigurował taką samą sieć laboratoryjną złożoną z 2-3 routerów Cisco 4221, 2-3 przełączników Cisco Catalyst 2960 oraz 2 firewalli ASA 5506-X 2 lub 3 komputerów PC wraz z wymaganym oprogramowaniem.
- Jako godzinę szkolenia przyjmuje się 45 minut.
- Walidacja będzie realizowana na ostatnich zajęciach w postaci:
 - egzaminu teoretycznego według międzynarodowych standardów szkolenia Cisco Network Security,
 - egzaminu praktycznego polegającego na projektowaniu, konfiguracji, testowaniu sieci wskazanej przez egzaminatora z uprawnieniami Cisco, także według ogólnoświatowej metodyki Network Academy.

- Opłata za usługę pokrywa wszystkie koszty, w tym: walidację, egzaminy podstawowy i poprawkowy oraz wydanie certyfikatów.

Szkolenie adresowane jest dla osób fizycznych lub pracowników firm:

- pracujących w branży sieciowej, pragnących poszerzyć lub uzupełnić wiedzę za zakresu realizacji poufności informacji przesyłanych przez sieć Internet oraz przeciwdziałania cyberatakam,
- operatorskich (inżynierów sieci), którzy zamierzają pozyskać umiejętności związane z zabezpieczeniem infrastruktury IT firmy (CyberSEC),
- zainteresowanych wdrażaniem tuneli VPN oraz bezpiecznego dostępu zdalnego do infrastruktury firmowej.
- chcących poszerzyć lub uporządkować wiedzę i umiejętności dotyczące zabezpieczenia sieci i urządzeń Cisco, tj. przełączników, routerów, firewalli,
- działów IT zarządzających infrastrukturą teleinformatyczną,
- pracujących na stanowiskach informatyka w MŚP, świadomych poziomu zagrożenia cyberprzestępczością,
- chcących uzupełnić wiedzę i kwalifikacje z zakresu szeroko pojętego bezpieczeństwa sieci korporacyjnych i kampusowy,
- planujących przebranżowienie wewnątrz firmy na stanowiska typu CyberSEC.

charakterystyka zajęć:

W - wykład

L - laboratorium

E - egzamin

Transformacja cyfrowa / zielone kompetencje

Szkolenie Cisco Network Security wpisuje się w koncepcję zielonych kompetencji ponieważ nowoczesne technologie komunikacyjne są rdzeniem transformacji cyfrowej, niezbędnej do faktycznej realizacji czystych oraz niskoemisyjnych technologii. Technologie komunikacyjne kursu Network Security umożliwiają firmom TRANSFORMACJĘ CYFROWA, która wprost pozwoli:

- skrócić czas realizacji procesów,
- na zarządzanie informacją,
- wprowadzać nowe produkty i usługi szybciej i taniej,
- zautomatyzować i przyspieszyć procesy w firmie,
- uzyskać przewagę konkurencyjną w stosunku do innych firm,
- łatwiej współpracować z dostawcami, klientami, partnerami
- sprawną obsługę klientów
- zajmować mniej powierzchni magazynowej, szaf i dokumentów
- lepiej chronić firmowe dane (CyberSecurity),

Nabyte przez uczestników szkolenia kompetencje cyfrowe wpisują się w Europejską Ramę Kompetencji Cyfrowych dla Obywateli (DigComp 2.2), w szczególności:

Obszar 2: Komunikacja i współpraca (2.1, 2.6)

Obszar 4: Bezpieczeństwo (4.1 / 4.4)

Obszar 5: Rozwiązywanie problemów (5.1 / 5.3)

Uznawanie kwalifikacje

Kurs Cisco Network Security jest rozpoznawalnym i cenionym kursem sieciowym na świecie. Kurs Network Security jest realizowany w strukturze edukacyjnej Cisco Networking Academy, która działa na świecie od ponad 20 lat i zrzesza ponad **11 700** akademii lokalnych w **190** krajach. Proces dydaktyczny jest identyczny na całym świecie, ponieważ Cisco Networking Academy ustandaryzowało szczegółowo proces dydaktyczny, dostarczając jednolite w skali świata: (1) wykłady, (2) instrukcje laboratoryjne, (3) środowisko realizacji kursu – netacad.com, (4) narzędzie symulacyjne Packet Tracer, (5) pliki symulacyjne z wbudowanym mechanizmem weryfikacyjnym. Na końcu procesu realizowana jest ujednolicona walidacja osiągniętych efektów kształcenia, która jest procesem zautomatyzowanym, przez co nie podlega ewentualnym wpływom ludzkim. Walidację nadzoruje egzaminator, który nie prowadził zajęć z daną grupą uczestników.

Fundacja ALTERnacja została pozytywnie zweryfikowana merytorycznie i na podstawie umowy z Cisco Networking Academy, będącą częścią Cisco Systems, Inc. z siedzibą w San Jose, otrzymała uprawnienia walidatora i wystawcy certyfikatów uzyskania wymaganych przez system kompetencji z zakresu kursów: CCNA, Network Security, CCNP etc. System walidacyjny efektów uczenia realizowany jest globalnie, na poziomie międzynarodowym. Wyniki walidacji są automatycznie generowane przez dedykowany system i dostarczane uczestnikowi jako ocena wiedzy i umiejętności. Pozytywna walidacja kwalifikacji i wydanie certyfikatu następuje dla uczestników, którzy otrzymali wymaganą sumę punktów z egzaminu. Na mocy umowy z Cisco Fundacja ALTERnacja posiada uprawnienia do umieszczania własnego logo obok logo Cisco Networking Academy jako instytucji certyfikującej. [Dot. 3.1.2.1 karty usługi 4) i 5)].

Harmonogram

Liczba pozycji harmonogramu: 39

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 39 Securing Networks (W)	Piotr Żmudziński	04-09-2026	16:30	18:00	01:30	Nie
2 z 39 Network Threats (W)	Piotr Żmudziński	04-09-2026	18:15	19:45	01:30	Nie
3 z 39 Network Threats (L)	Piotr Żmudziński	04-09-2026	20:00	21:30	01:30	Nie
4 z 39 Mitigating Threats (W)	Piotr Żmudziński	11-09-2026	16:30	18:00	01:30	Nie
5 z 39 Secure Device Access (W)	Piotr Żmudziński	11-09-2026	18:15	19:45	01:30	Nie
6 z 39 Secure Device Access (W)	Piotr Żmudziński	11-09-2026	20:00	21:30	01:30	Nie
7 z 39 Assign Administrative Roles (W)	Piotr Żmudziński	18-09-2026	16:30	18:00	01:30	Nie
8 z 39 Device Monitoring and Management (L)	Piotr Żmudziński	18-09-2026	18:15	19:45	01:30	Nie
9 z 39 Authentication, Authorization, and Accounting (W)	Piotr Żmudziński	18-09-2026	20:00	21:30	01:30	Nie

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
10 z 39 Authentication, Authorization, and Accounting (L)	Piotr Żmudziński	25-09-2026	16:30	18:00	01:30	Nie
11 z 39 Access Control Lists (L)	Piotr Żmudziński	25-09-2026	18:15	19:45	01:30	Nie
12 z 39 Firewall Technologies (W)	Piotr Żmudziński	25-09-2026	20:00	21:30	01:30	Nie
13 z 39 Zone-Based Policy Firewalls cz.1 (L)	Piotr Żmudziński	02-10-2026	16:30	18:00	01:30	Nie
14 z 39 Zone-Based Policy Firewalls cz.2 (L)	Piotr Żmudziński	02-10-2026	18:15	19:45	01:30	Nie
15 z 39 Zone-Based Policy Firewalls cz.3 (L)	Piotr Żmudziński	02-10-2026	20:00	21:30	01:30	Nie
16 z 39 IPS Technologies (W)	Piotr Żmudziński	09-10-2026	16:30	18:00	01:30	Nie
17 z 39 IPS Operation and Implementation (W)	Piotr Żmudziński	09-10-2026	18:15	19:45	01:30	Nie
18 z 39 Endpoint Security (W)	Piotr Żmudziński	09-10-2026	20:00	21:30	01:30	Nie
19 z 39 Layer 2 Security Considerations (L)	Piotr Żmudziński	16-10-2026	16:30	18:00	01:30	Nie

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
20 z 39 Layer 2 Security Considerations (L)	Piotr Żmudziński	16-10-2026	18:15	19:45	01:30	Nie
21 z 39 Cryptographic Services (W)	Piotr Żmudziński	16-10-2026	20:00	21:30	01:30	Nie
22 z 39 Basic Integrity and Authenticity (W)	Piotr Żmudziński	23-10-2026	16:30	18:00	01:30	Nie
23 z 39 Public Key Cryptography (W)	Piotr Żmudziński	23-10-2026	18:15	19:45	01:30	Nie
24 z 39 VPNs (W)	Piotr Żmudziński	23-10-2026	20:00	21:30	01:30	Nie
25 z 39 Implement Site-to-Site IPsec VPNs with CLI (L)	Piotr Żmudziński	30-10-2026	16:30	18:00	01:30	Nie
26 z 39 Implement Site-to-Site IPsec VPNs with CLI (L)	Piotr Żmudziński	30-10-2026	18:15	19:45	01:30	Nie
27 z 39 Introduction to the ASA (W)	Piotr Żmudziński	30-10-2026	20:00	21:30	01:30	Nie
28 z 39 Introduction to the ASA (L)	Piotr Żmudziński	06-11-2026	16:30	18:00	01:30	Nie
29 z 39 Introduction to the ASA (L)	Piotr Żmudziński	06-11-2026	18:15	19:45	01:30	Nie
30 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	06-11-2026	20:00	21:30	01:30	Nie

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
31 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	13-11-2026	16:30	18:00	01:30	Tak
32 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	13-11-2026	18:15	19:45	01:30	Tak
33 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	13-11-2026	20:00	21:30	01:30	Tak
34 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	20-11-2026	16:30	18:00	01:30	Tak
35 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	20-11-2026	18:15	19:45	01:30	Tak
36 z 39 Network Security Testing (L)	Piotr Żmudziński	20-11-2026	20:00	21:30	01:30	Tak
37 z 39 Ćwiczenie podsumowujące (L)	Piotr Żmudziński	27-11-2026	16:30	18:00	01:30	Nie
38 z 39 Egzamin (E)	-	27-11-2026	18:15	19:45	01:30	Nie
39 z 39 Egzamin (E)	-	27-11-2026	20:00	21:30	01:30	Nie

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 400,00 PLN

Koszt przypadający na 1 uczestnika netto	6 400,00 PLN
Koszt osobogodziny brutto	82,05 PLN
Koszt osobogodziny netto	82,05 PLN
W tym koszt walidacji brutto	200,00 PLN
W tym koszt walidacji netto	200,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Piotr Żmudziński

Przez ostatnie 5 lat: (1) wykładowca akademicki na Wydziale Informatyki Uniwersytetu Kazimierza Wielkiego, (2) przeprowadził ponad 3.000 zajęć dydaktycznych. Przez ostatnie 5 lat trener i egzaminator njanowszych wersji kursów Cisco: CCNA, CCNP, Network Security, zrealizował 12 szkoleń Cisco:

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestnik szkolenia otrzyma:

- dostęp do platformy elearningowej netacad.com, także po zakończeniu szkolenia. W netacad.com dostępne są kompletne materiały e-learningowe do kursu,
- dostęp do własnej platformy Fundacji ALTERnacja celem pobierania zadań symulacyjnych,
- imienną licencję na oprogramowanie symulacyjne Packet Tracer, wykorzystywaną do symulacji sieci,
- dodatkowe, autorskie materiały edukacyjne, wykraczające poza ramy szkolenia Cisco Network Security.

Warunki uczestnictwa

Przystępując do kursu Cisco Network Security, uczestnik powinien posiadać podstawową wiedzę związaną z działaniem sieci oraz wiedzy związanej z protokołami sieci komputerowych na poziomie odpowiadającym sem.1 i sem.2 kursu Cisco CCNA. Nie jest wymagane posiadanie certyfikatu ukończenia szkolenia CCNA.

Szkolenie przeznaczona dla uczestników z dowolnego programu dofinansowania:

- Kierunek - Rozwój
- Opolskie stawia na rozwój
- Bon na szkolenie w subregionie suwalskim
- Bon na szkolenie w subregionie łomżyńskim
- PROFESJONALNE KADRY PODLASIA - wsparcie rozwoju kwalifikacji mieszkańców subregionu białostockiego oraz innych projektów z terenu Polski.
- innych projektów.

Dla projektu "Usługi rozwojowe dla mieszkańców podregionu leszczyńskiego" wymagana jest minimalna frekwencja 80%.

Zawarto umowę z WUP w Toruniu w ramach projektu Kierunek – Rozwój

Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projekt

Informacje dodatkowe

Jako godzinę szkolenia przyjmuje się godzinę dydaktyczną tj. 45 minut. Przerwy między w zajęciach nie są wliczane do czasu szkolenia.

Kwalifikacja lub kompetencja związana z cyfrową transformacją. Zawierza także treści dot. zielonych technologii.

Podatnik zwolniony z podatku VAT na podstawie art. 43 ust. 1 pkt 29c ustawy o podatku od towarów i usług.

Szkolenie związane jest z UMIEJĘTNOŚCIAMI CYFROWYMI na poziomie średnio zaawansowanym, związane z przesyłaniem informacji poprzez sieć komputerową / Internet oraz podstawami bezpieczeństwa przesyłania informacji tj. cybersecurity,

Kurs wpisuje się w zakres przedmiotowy Inteligentnych Specjalizacji Pomorza wg. zał1 uchwały 591/549/24 Zarządu Województwa Pomorskiego z dnia 21.05.2025. ISP 2 - punkt 2 "Przestrzenie i systemy inteligentne" podpunkt, punkt 4 "Sztuczna Inteligencja oraz zaawansowane przetwarzanie i cyberbezpieczeństwo danych" podpunkt c.

Warunki techniczne

Aby uczestniczyć w zajęciach zdalnych kursu Cisco CCNA, uczestnik powinien dysponować typowym komputerem stacjonarnym lub laptopem o minimalnych parametrach:

- łącze internetowe dowolnej technologii (także LTE) o przepustowości przynajmniej 4 Mbit/s,
- procesor Intel i3 lub równoważny albo lepszy,
- pamięć RAM: 8 GB lub więcej,
- wolne miejsce na dysku: przynajmniej 500 MB,
- kamera i mikrofon.
- Zdalna część szkolenia będzie odbywała się

Adres

ul. Mikołaja Kopernika 1/108

85-074 Bydgoszcz

woj. kujawsko-pomorskie

Zajęcia ze sprzętem sieciowym będą realizowane w laboratorium sieciowym Wydziału Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy.

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

- Obiekt przystosowany dla osób z niepełnosprawnościami: winda, podjazdy, brak progów.

Kontakt



Piotr Żmudziński

E-mail piotr@alternacja.pl

Telefon (+48) 695 616 100