



Inżynier bezpieczeństwa sieci MikroTik MTCSE (MikroTik Certified Security Engineer) (szkolenie z egzaminem)

Numer usługi 2026/08/01/134180/3724581

6 800,00 PLN brutto

6 800,00 PLN netto

100,00 PLN brutto/h

100,00 PLN netto/h

332,00 PLN cena rynkowa ⓘ

CS EDU IDET

SPÓŁKA Z

OGRANICZONĄ

ODPOWIEDZIALNOŚĆ

CIĄ

★★★★★ 4,8 / 5

134 oceny

🏠 Usługa szkoleniowa

📄 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 68:00 h

📅 21.08.2026 do 20.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikatory projektów	Małopolski Pociąg do kariery
Grupa docelowa usługi	Obecni oraz przyszli administratorzy bezpieczeństwa sieci komputerowych, wszyscy pracownicy, którzy w zakresie swoich obowiązków mają zadania związane z zarządzaniem i utrzymaniem bezpieczeństwa sieci komputerowych zbudowanych w oparciu o sprzęt firmy MikroTik oraz tacy którzy chcą poznać metody zdalnego zarządzania i monitorowania zużycia energii urządzeń końcowych podłączonych do szkieletowego sprzętu sieciowego. Jak również metody bezpiecznego dostępu do wewnątrz sieci celem włączania i wyłączania zasilania końcowych urządzeń takich jak access pointy czy kamery sieciowe za pomocą nowoczesnej metody zasilania wyłącznie kablem sygnałowym bez potrzeby doprowadzania do nich odrębnego zasilania. Co umożliwia centralizację oraz zdalne bezpieczne i inteligentne zarządzanie zasilaniem; włączanie urządzeń tylko wtedy gdy rzeczywiście są używane (np. automatyczne wyłączanie urządzeń w nocy gdy i tak nie byłyby używane). Szkolenie adresowane jest do wszystkich projektów ogólnopolskich.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	19-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Cel

Cel edukacyjny

Nabycie umiejętności administrowania siecią komputerową wyposażoną w sprzęt MikroTik w firmach, zakładach przemysłowych, jednostkach handlowych i administracyjnych, organizacjach, instytucjach i placówkach planujących wdrożyć bezpieczny zdalny monitoring umożliwiający inteligentne zarządzanie energią i automatyzację umożliwiającą redukcję jej zużycia.

Celem szkolenie jest zdobycie wiedzy i umiejętności w zakresie bezpieczeństwa sieci komputerowych opartych o energooszczędne urządzenia MikroTik.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przeprowadza zaawansowaną konfigurację Firewall	Wybór właściwej odpowiedzi na teście końcowym w pytaniach dotyczących zaawansowanej konfiguracji Firewall na urządzeniu sieciowym użytym w danym scenariuszu.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje Tunele L2TP	Rozróżnia i wymienia w odpowiedniej kolejności kroki jakie należy wykonać celem skonfigurowania i zestawienia Tunelu L2TP	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje Tunele SSTP	Rozróżnia i wymienia w odpowiedniej kolejności kroki jakie należy wykonać celem prawidłowego skonfigurowania a następnie zestawienia Tunelu SSTP	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje Tunele IPSec	Rozróżnia, wylicza w odpowiedniej kolejności kroki jakie należy wykonać aby prawidłowego skonfigurować i zestawić połączenie Tunelowane IPSec	Test teoretyczny z wynikiem generowanym automatycznie
Przeprowadza konfigurację Port Knocking	Wymienia kroki niezbędne do skonfigurowania Port Knocking na urządzeniu a następnie łączy się do urządzenia na podstawie wcześniej skonfigurowanej sekwencji.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje Zasady bezpieczeństwa sieci komputerowych	Rozróżnia otwarte porty dostępu do urządzenia i zamyka nieużywanie pozostawiając i zabezpieczając tylko te wymagane w danym scenariuszu.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia metody ograniczenia dostępu do zarządzania routerem	Ogranicza dostęp do routera tylko dla wymaganych lokalizacji zamykając dostęp z pozostałych pozostawiając otwarte na świat tylko wymagane w danym scenariuszu porty.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje protokół POE (Power over Ethernet)	Weryfikacja czy uczestnik potrafi zarządzać oszczędzaniem energii końcówek podpiętych do szkieletowego urządzenia sieciowego tj. odszukać i włączyć odpowiednią opcję na porcie urządzenia sieciowego celem zarządzania energią końcówek podpiętych do jego portów (zdalnie wyłączyć i włączyć zasilanie urządzenia końcowego podpiętego do jego portu) a następnie sprawdzić czy urządzenie jest osiągalne czy nie. Podobne operacje wykonywać dla grupy portów i automatyzować je za pomocą skryptów.	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://mikrotik.com>

Strona internetowa Instytucji Walidującej: <https://mikrotik.com>

Informacje

Nazwa Podmiotu prowadzącego walidację	MikroTik
Nazwa Podmiotu certyfikującego	MikroTik

Program

Zapoznanie z systemem stosowanym w urządzeniach sieciowych MikroTik (teoria + praktyka)

Praktyczne ćwiczenia obejmujące budowanie topologii sieciowych z wykorzystaniem urządzeń sieciowych Mikrotik.

Ćwiczenia obejmują m.in:

- Konfigurowanie Firewall
- Konfigurowanie Port knocking
- Konfigurowanie SSH forwarding
- Konfigurowanie tuneli L2TP
- Konfigurowanie tuneli IPSec
- Konfigurowanie tuneli SSTP
- Konfigurowanie certyfikatów oraz kluczy dla połączeń VPN.
- Konfigurowanie zabezpieczeń przeciw atakom m. in. na DHCP.

Zdalny dostęp do urządzeń w celu obserwacji statusów portów i obsługi na nich funkcji "ECO".

Konfiguracja portów w taki sposób aby dostosować prędkość do realnej przepustowości (tzn. na urządzeniach wymagających minimalnej przepustowości zredukować prędkość portu do minimalnej np. 10Mbps co w znaczący sposób wpłynie na zmniejszenie zużycia energii (gdy funkcja zostanie zastosowana dla kilkunastu bądź kilkudziesięciu urządzeń).

Zalecane (nie obowiązkowe z uwagi na to, że ćwiczenia wykonywane będą na maszynach wirtualnych) aby na czas szkolenia uczestnik posiadał dowolne fizyczne urządzenie MikroTik (np. hAP lite RB941-2nD)

Istnieje możliwość wypożyczenia takiego urządzenia na czas zajęć przed rozpoczęciem szkolenia.

Egzamin:

- trwa 60 minut
- prowadzony jest w języku angielskim
- jest to test jedno lub wielokrotnego wyboru (w zależności od pytania)
- próg zdawalności to 60%
- przed rozpoczęciem właściwego egzaminu uczestnik przystąpi do egzaminu próbnego.

Kwalifikacja potwierdzona zostanie międzynarodowym certyfikatem. Celem szczegółowym szkolenia jest zapoznanie z funkcjami systemu RouterOS umożliwiającymi budowę bezpiecznej sieci komputerowej.

Wiedza nabyta podczas szkolenia znajdzie zastosowanie przy tworzeniu topologii sieciowych bezpiecznych sieci komputerowych opartych o zarządzane z wiersza polecenia urządzenia sieciowe firmy MikroTik.

Podczas szkolenia uczestnicy nabędą wiedzę jak skonfigurować bezpieczną sieć komputerową z zastosowaniem opartą o zarządzane z wiersza polecenia urządzenia sieciowe firmy MikroTik.

Uczestnik przetestuje działanie bezpiecznej sieci komputerowej w najpopularniejszych symulatorach pozwalających odwzorować produkcyjną sieć komputerową opartą o urządzenia różnych producentów w środowisku testowym.

Wykonywane podczas szkolenia ćwiczenia praktyczne oparte są o najpopularniejsze scenariusze z codziennej pracy administratora sieci. Dzięki specjalnej wyizolowanej publicznej testowej sieci na cele szkoleniowe uczestnicy zabezpieczą router brzegowy, skonfigurują sieć a następnie przetestują ją pod kątem bezpieczeństwa w dokładnie taki sam sposób w jaki wykonuje się to w rzeczywistej firmowej sieci komputerowej. W ramach szkolenia istnieje możliwość uzyskania pierwszego podstawowego certyfikatu MikroTik Certified Network Associate oraz certyfikatu inżynierskiego MikroTik Certified Security Engineer.

W przypadku gdy Uczestnik jest już posiadaczem certyfikatu MTCNA słuchacz powinien:

posiadać podstawową wiedzę na temat projektowania adresacji IPv4 w sieciach komputerowych,

potrafić stosować maskę podsieci odpowiedniej długości w zależności od aktualnych i przyszłych potrzeb ilościowych urządzeń w sieci, wykonywać konwersje między systemami liczbowymi (dwójkowym, dziesiętnym i szesnastkowym), posiadać wiedzę jak zbudować prostą sieć komputerową w oparciu o niezarządzane urządzenia sieciowe.

Jeśli Uczestnik posiada już certyfikat MTCNA w ramach usługi ma możliwość jego odnowienia.

W celu efektywnego uczestnictwa w szkoleniu słuchacz powinien posiadać już powyższą wiedzę a warunkiem obligatoryjnym podejścia do egzaminu MTCSE jest posiadanie certyfikatu MTCNA (jedno podejście do certyfikatu inżynierskiego oraz jedno podejście/odnowienie certyfikatu podstawowego jest w cenie usługi)

Przed przystąpieniem do egzaminu końcowego uczestnik przystąpi do egzaminu próbnego.

Uczestnicy, którzy wcześniej już go posiadali zdany egzamin MTCNA odnowią certyfikację. Koszt egzaminu zawarty w cenie usługi.

Po ukończeniu szkolenia uczestnicy przystąpią do egzaminu inżynierskiego bezpieczeństwa sieci MikroTik. Koszt egzaminu zawarty w cenie usługi.

Po ukończeniu szkolenia uczestnicy przystąpią do egzaminu inżyniera bezpieczeństwa sieci MikroTik.

Usługa realizowana w formie zdalnej (zdalny dostęp i zarządzanie bezpieczną siecią komputerową) [przy użyciu sieciowych systemów operacyjnych oraz sprzętu sieciowego w postaci maszyn wirtualnych oraz wirtualnych połączeń między nimi]

W związku z tym, że usługa prowadzona jest w formie zdalnej Uczestnik powinien posiadać:

- najnowszą wersję przeglądarki Google Chrome.

- łącze internetowe o przepustowości co najmniej 2 Mbps / 1 Mbps z odblokowanymi portami 22, 23, 69, 3800, 5901-5908, 6101-6108, 6151-6158 na ruch wychodzący.

Linki z zaproszeniami do wideokonferencji będą wysyłane na adresy e-mail uczestników 15 minut przed rozpoczęciem spotkania.

Certyfikat w Klasyfikacji Zawodów i Specjalności:

Szczegółowa nazwa kwalifikacji zawodowej: **Inżynier systemów i sieci komputerowych (252302)**

Nazwa jednostki certyfikującej (egzaminującej): **MikroTik**

Nazwa certyfikatu: **MikroTik Certified Security Engineer**

Jednostką rozliczeniową jest godzina lekcyjna dydaktyczna (45 min).

Usługa obejmuje 68 godzin dydaktycznych (po 45 min) stąd w harmonogramie

51 godzin lekcyjnych

to

68 godzin dydaktycznych

68 godzin dydaktycznych lekcyjnych to 51 godzin zegarowych.

68 godzin dydaktycznych * 45/60 = 51 godzin zegarowych.

W karcie umieszczono informację, że jednostką rozliczeniową jest godzina lekcyjna (dydaktyczna tj. 45 min)

Czas przeznaczony na egzamin (walidację) jest wliczony do czasu trwania usługi.

Przerwy nie występują i nie są wliczone w czas usługi rozwojowej.

Gdyby wystąpiła w harmonogramie jako przerwę należałoby traktować czas pomiędzy poszczególnymi blokami, który w ogóle nie jest wpisywany w harmonogram.

Przykładowo gdyby jeden blok kończył się o godzinie 13.30 a kolejny zaczynał o 13.45 to ten czas od 13.30 do 13.45 w ogóle nie jest byłby uwzględniany w harmonogramie i nie liczyłby się do czasu trwania usługi.

Liczba godzin usługi to 68 godzin dydaktycznych (lekcyjnych) na co składa się :

- część teoretyczna szkolenia

- część praktyczna szkolenia

- część egzaminacyjna

*Co daje w sumie 68 godzin dydaktycznych tj. 51 godzin zegarowych (68 *45min/60min) = 51*

(w polu program usługi przedstawiono szczegółowe wyliczenie) W polu liczba godzin usługi wskazano 68. Liczba zsumowanych godzin w harmonogramie to 51 ponieważ harmonogram zlicza godziny zegarowe.

Liczba godzin w podziale na zajęcia praktyczne i teoretyczne

Usługa obejmuje:

- 12 godzin teoretycznych (szkolenia)
- 50 godzin praktycznych (szkolenia)
- 4 godziny egzaminu

(jednostka godzinowa liczona jako godzina lekcyjna tj. 45 min)

Razem 68 godzin lekcyjnych (dydaktycznych) = 51 godzin zegarowych

W sumarycznej liczbie godzin uwzględniono walidację (egzamin).

Liczba godzin uwzględniająca liczbę godzin procesu kształcenia oraz walidacji: 68 godzin dydaktycznych.

Usługa realizowana w godzinach dydaktycznych.

Infrastruktura sieciowa zbudowana na urządzeniach firmy MikroTik ma mniejsze zużycie energii dzięki zastosowaniu nowych technologii.

Ponadto omówione zostaną scenariusze wyeliminowania klasycznych zasilaczy sieciowych a zasilanie zostanie zastąpione technologią POE czyli zasilaniu za pomocą kabla sygnałowego.

Nie używane urządzenia mogą zostać zdalnie wyłączone dzięki tej technologii co znacznie wpłynie na oszczędność energii.

Dzięki sieci zbudowanej na nowoczesnych urządzeniach sieciowych MikroTik można zdalnie monitorować infrastrukturę dzięki czemu urządzenie może być zasilane z paneli fotowoltaicznych.

A skrypty informujące o rozładowaniu akumulatora w przypadku dłuższego czasu braku słońca pozwalają odpowiednio szybko zareagować aby przełączyć na klasyczne sieciowe zasilanie dla fotowoltaiki aby nie dopuścić do całkowitego rozładowania baterii.

Całkowite rozładowanie powoduje nieodwracalne uszkodzenie instalacji fotowoltaicznej stąd opanowanie zdalnego zarządzania siecią w oparciu o sprzęt MikroTik-a jest tak ważne dla utrzymania sprawności instalacji i sprawnego reagowania na awarie.

Urządzenia umożliwiają również reakcję nawet w przypadku awarii Internetu stacjonarnego ponieważ wyposażone są w moduły do Internetu mobilnego dzięki któremu instalacje fotowoltaiczną można monitorować nawet w przypadku awarii lokalnego dostawcy Internetu.

Nowe technologie użyte w sprzęcie MikroTik pozwalają zrealizować wiele scenariuszy dla zapewniania stabilności i bezawaryjności działania instalacji fotowoltaicznych.

Same urządzenia ze względu na niski pobór prądu mogą być zasilane również z powerbanków (również takich na małe panele fotowoltaiczne), portów USB laptopów czy akumulatorów samochodowych.

Obszar technologiczny szkolenia:

Technologie informacyjne i telekomunikacyjne

4.1. Technologie telekomunikacyjne

4.2 Technologie informacyjne

4.6 Bezpieczeństwo informacji

Harmonogram

Liczba pozycji harmonogramu: 27

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 27 Zabezpieczanie dostępu do routera, MikroTik Port knocking, SSH forwarding (w kontekście oszczędności energii urządzeń, metod monitorowania) [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	21-08-2026	18:00	22:30	04:30
2 z 27 -	Przerwa	-	21-08-2026	22:30	23:45	01:15
3 z 27 Zabezpieczanie dostępu do routera, MikroTik Port knocking, SSH forwarding (w kontekście oszczędności energii urządzeń, metod monitorowania) [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	22-08-2026	17:15	21:45	04:30
4 z 27 -	Przerwa	-	22-08-2026	21:45	23:00	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 27 Tunele; L2TP, SSTP, klucze, certyfikaty zabezpieczające połączenia VPN w kontekście zdalnego zarządzania energią i wyłączania nieaktywnych urządzeń protokołem POE) [fz] (prezentacja + samodzielne ćwi)	Zajęcia	TADEUSZ RUCHLEWICZ	23-08-2026	18:14	22:44	04:30
6 z 27 -	Przerwa	-	23-08-2026	22:44	23:59	01:15
7 z 27 Tunele; L2TP, SSTP, klucze, certyfikaty zabezpieczające połączenia VPN w kontekście zdalnego zarządzania energią i wyłączania nieaktywnych urządzeń protokołem POE) [fz] (prezentacja + samodzielne ćwi)	Zajęcia	TADEUSZ RUCHLEWICZ	24-08-2026	18:14	22:44	04:30
8 z 27 -	Przerwa	-	24-08-2026	22:44	23:59	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 27 Tunele; L2TP, SSTP, klucze, certyfikaty zabezpieczające połączenia VPN w kontekście zdalnego zarządzania energią i wyłączania nieaktywnych urządzeń protokołem POE) [fz] (prezentacja + samodzielne ćwic)	Zajęcia	TADEUSZ RUCHLEWICZ	25-08-2026	18:14	22:44	04:30
10 z 27 -	Przerwa	-	25-08-2026	22:44	23:59	01:15
11 z 27 Tunele; IPSec, [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	26-08-2026	18:14	22:44	04:30
12 z 27 -	Przerwa	-	26-08-2026	22:44	23:59	01:15
13 z 27 Tunele; IPSec, [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	27-08-2026	18:14	22:44	04:30
14 z 27 -	Przerwa	-	27-08-2026	22:44	23:59	01:15
15 z 27 Tunele; VPN (2 i 3 warstwy), [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	28-08-2026	18:14	22:44	04:30
16 z 27 -	Przerwa	-	28-08-2026	22:44	23:59	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 27 Tunele; IPSec, [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	29-08-2026	18:14	21:14	03:00
18 z 27 -	Walidacja	-	29-08-2026	21:14	22:44	01:30
19 z 27 -	Przerwa	-	29-08-2026	22:44	23:59	01:15
20 z 27 Tunele; VPN (2 i 3 warstwy), [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	30-08-2026	18:14	22:44	04:30
21 z 27 -	Przerwa	-	30-08-2026	22:44	23:59	01:15
22 z 27 Firewall, ochrona przed atakami m in na serwer DHCP [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	31-08-2026	09:45	11:30	01:45
23 z 27 Egzamin próbny [forma zdalna] (test teoretyczny z wynikiem generowanym automatycznie)	Zajęcia	TADEUSZ RUCHLEWICZ	31-08-2026	11:30	12:30	01:00
24 z 27 -	Walidacja	-	31-08-2026	12:30	14:00	01:30
25 z 27 -	Przerwa	-	31-08-2026	14:00	14:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 27 Zabezpieczanie dostępu do routera, MikroTik Port knocking, SSH forwarding (w kontekście oszczędności energii urządzeń, metod monitorowania) a) [forma zdalna] (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	20-09-2026	18:14	22:44	04:30
27 z 27 -	Przerwa	-	20-09-2026	22:44	23:59	01:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	68:00
w tym suma godzin zajęć	50:45
w tym suma godzin walidacji	03:00
w tym suma przerw	14:15
Suma godzin dydaktycznych bez przerw	71:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
Koszt przypadający na 1 uczestnika netto	6 800,00 PLN

Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN
W tym koszt walidacji brutto	2 000,00 PLN
W tym koszt walidacji netto	2 000,00 PLN
W tym koszt certyfikowania brutto	2 000,00 PLN
W tym koszt certyfikowania netto	2 000,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	68:00

Prowadzący

Liczba prowadzących: 1



1 z 1

TADEUSZ RUCHLEWICZ

Specjalność w zakresie administrowania systemami i sieciami komputerowymi.

Uprawnienia;
instruktorskie z zakresu Cisco Certified Network Associate (CCNA) (Akademia Górniczo-Hutnicza),
Cisco Certified Network Professional (CCNP) (Route, Switch, Troubleshoot) (WSiZ Rzeszów),
certyfikat Cisco CCNAv7 200-301.
certyfikat trenera MikroTik (Łotwa); instruktor z zakresu: MTCNA, MTCRE, MTCWE, MTCTCE,
MTCUME, MTCINE, MTCSE, MTCSEWE, certyfikat inżyniera MikroTik: MTCEWE.
Piętnastoletnie doświadczenie w pracy na stanowisku administratora sieci komputerowej Instytutu Informatyki Uniwersytetu Rzeszowskiego.
Pełnienie funkcji Koordynatora Lokalnej Akademii Cisco Uniwersytetu Rzeszowskiego.
Organizacja i prowadzenie autoryzowanych szkoleń Cisco Certified Network Associate Routing and Switching (CCNA R&S).
Organizacja i prowadzenie certyfikowanych szkoleń MikroTik Certified [Network Associate, (Routing, Wireless, Security, Traffic Control) Engineer].

Autor programu studiów podyplomowych: "Systemy i sieci komputerowe (Cisco Certified)" oraz szkolenia "Administrator sieci komputerowej (Cisco, MikroTik)" realizowanego na Uniwersytecie Rzeszowskim.

Absolwent Politechniki Rzeszowskiej; kierunek Informatyka; specjalność systemy i sieci

komputerowe - uzyskany stopień mgr inż.

Absolwent Uniwersytetu Rzeszowskiego: kierunek fizyka komputerowa - uzyskany stopień mgr.

Absolwent kwalifikacyjnych studiów podyplomowych praktyczne nauczanie zawodu w grupie przedmiotów elektryczno - elektronicznych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały edukacyjne z zakresu administrowania sieciami komputerowymi.

W ramach szkolenia uczestnik otrzymuje dostęp do materiałów edukacyjnych z zakresu administrowania sieciami komputerowymi, interaktywnych ćwiczeń praktycznych,

Usługa rozliczana w godzinach dydaktycznych (lekcyjnych) (po 45 min)

Warunki uczestnictwa

Do wzięcia udziału w szkoleniu wymagana jest podstawowa umiejętność obsługi komputera. Zalecane jest posiadanie pierwszego podstawowego certyfikatu MikroTik lub wiedza umożliwiająca jego uzyskanie.

W związku z tym, że usługa współfinansowana jest ze środków publicznych należy dokonać na nią zapisu w następujący sposób:

- należy zapisać się na usługę (w okresie rekrutacji) przy użyciu przydzielonego **ID wsparcia** (zapis bez ID wsparcia uniemożliwi uzyskanie dofinansowania)
- dokonać opłaty za usługę (na podstawie otrzymanej faktury zachowując dowód wpłaty do celów rozliczeniowych z operatorem) zgodnie umową dofinansowania.
- ocenić usługę po jej zakończeniu.
- dopełnić wszelkich formalności rozliczeniowych zgodnie z umową dofinansowania.

Informacje dodatkowe

Zalecane (nie obowiązkowe z uwagi na to, że ćwiczenia wykonywane będą na maszynach wirtualnych) aby na czas szkolenia uczestnik posiadał dowolne fizyczne urządzenie MikroTik (np. hAP lite RB941-2nD)

Po zakończonych zajęciach a przed egzaminem zostanie wykonane zdjęcie uczestnikom.

Wykonanie zdjęcia jest niezbędne do zamieszczenia platformie egzaminacyjnej i oznaczenia uczestników celem weryfikacji tożsamości przed przystąpieniem do egzaminu.

Podczas zajęć uczestnikom udostępnione zostanie środowisko pracy w postaci wirtualnych maszyn.

Cena usługi uwzględnia jedno podejście do pierwszego podstawowego egzaminu certyfikacyjnego MTCNA oraz jedno podejście do inżynierskiego egzaminu certyfikacyjnego MTCSE.

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Małopolski pociąg do kariery – sezon I”.

Warunki techniczne

platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

Teams lub poprzez przeglądarkę internetową za pomocą platformy Office365, oraz Google Hangouts do jednoczesnej prezentacji zawartości przez prowadzącego i uczestnika (wymagane konto na Gmail)

minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

Procesor taktowanie minimum 1.6 GHz , 2 rdzenie, Pamięć RAM min 4GB, Dysk twardy min 3GB wolnej przestrzeni dyskowej, Wyświetlacz rozdzielczość 1024x768 lub wyższa

niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

Teams lub przeglądarka internetowa (np. Google Chrome)

okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line:

Uczestnictwo odbywać się będzie poprzez aplikację Teams (autoryzacja za pomocą loginu i hasła, link nie jest wymagany), Link do dodatkowej aplikacji umożliwiającej jednoczesną prezentację przez trenera i uczestnika będzie ważny w okresie trwania szkolenia.

Łącze internetowe umożliwiające transmisję video (o parametrach co najmniej 2Mbps)

Kontakt



TADEUSZ RUCHLEWICZ

E-mail tadeusz.ruchlewicz@gmail.com

Telefon (+48) 604 922 386