



Inżynier bezpieczeństwa sieci MikroTik (indywidualnie) (szkolenie) - Małopolski pociąg do kariery – sezon I [forma zdalna] (TERMINY REALIZACJI DO USTALENIA)

Numer usługi 2026/06/17/134180/3631946

3 600,00 PLN brutto
 3 600,00 PLN netto
 120,00 PLN brutto/h
 120,00 PLN netto/h
 332,00 PLN cena rynkowa ⓘ

CS EDU IDET

SPÓŁKA Z

OGRANICZONĄ

ODPOWIEDZIALNOŚĆ

CIĄ

★★★★★ 4,8 / 5

124 oceny

📄 Usługa szkoleniowa

📄 zdalna w czasie rzeczywistym

📄 Zajęcia indywidualne

🕒 30:00 h

📅 20.07.2026 do 24.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikatory projektów	Małopolski Pociąg do kariery
Grupa docelowa usługi	<p>Obecni oraz przyszli administratorzy sieci komputerowych, wszyscy pracownicy, którzy w zakresie swoich obowiązków mają zadania związane z zarządzaniem i utrzymaniem sieci komputerowych zbudowanych w oparciu o sprzęt firmy MikroTik.</p> <p>Usługa również adresowana dla Uczestników Projektu "Małopolski pociąg do kariery - sezon 1" i/lub dla Uczestników Projektu "Nowy start w Małopolsce z EURESem"</p>
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1
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

Nabycie wiedzy umożliwiającej podjęcie pracy na stanowisku administratora sieci komputerowej wyposażonej w sprzęt MikroTik w firmach, zakładach przemysłowych, jednostkach handlowych i administracyjnych, organizacjach lub innych

instytucjach i placówkach, w których wykorzystuje się sieć komputerową i stosowne dla danej instytucji oprogramowanie.

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

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
charakteryzuje zasady bezpieczeństwa sieci komputerowych definiuje zasady i metody ograniczenia dostępu do zarządzania routerem konfiguruje Port Knocking konfiguruje zaawansowane opcje Firewall stosuje tunele L2TP stosuje tunele SSTP stosuje tunele IPSec	Wykonanie pre-testu (przed rozpoczęciem szkolenia) i post-testu (po ukończeniu szkolenia)	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

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.

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.

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 celu efektywnego uczestnictwa 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.

W celu efektywnego uczestnictwa w szkoleniu słuchacz powinien posiadać już powyższą wiedzę jednak istnieje możliwość uzupełnienia wiedzy na platformie do samodzielnej nauki (z zakresu sieci komputerowych) do której uczestnik otrzymuje dostęp w ramach uczestnictwa w usłudze

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.

Jednostką rozliczeniową jest godzina lekcyjna (45 min)

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Zabezpieczanie dostępu do routera, MikroTik Port knocking, SSH forwarding [forma zdalna]	Zajęcia	TADEUSZ RUCHLEWICZ	20-07-2026	08:00	12:30	04:30
2 z 11 -	Przerwa	-	20-07-2026	12:30	13:45	01:15
3 z 11 Zabezpieczanie dostępu do routera, MikroTik Port knocking, SSH forwarding [forma zdalna]	Zajęcia	TADEUSZ RUCHLEWICZ	21-07-2026	08:00	12:30	04:30
4 z 11 -	Przerwa	-	21-07-2026	12:30	13:45	01:15
5 z 11 Tunele; L2TP, IPSec, SSTP, klucze, certyfikaty zabezpieczające połączenia VPN [forma zdalna]	Zajęcia	TADEUSZ RUCHLEWICZ	22-07-2026	08:00	12:30	04:30
6 z 11 -	Przerwa	-	22-07-2026	12:30	13:45	01:15
7 z 11 Tunele; L2TP, IPSec, SSTP, klucze, certyfikaty zabezpieczające połączenia VPN [forma zdalna]	Zajęcia	TADEUSZ RUCHLEWICZ	23-07-2026	08:00	12:30	04:30
8 z 11 -	Przerwa	-	23-07-2026	12:30	13:45	01:15
9 z 11 Firewall, ochrona przed atakami m in na serwer DHCP [forma zdalna]	Zajęcia	TADEUSZ RUCHLEWICZ	24-07-2026	08:00	12:30	04:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 11 -	Przerwa	-	24-07-2026	12:30	13:45	01:15
11 z 11 -	Walidacja	TADEUSZ RUCHLEWICZ	24-07-2026	13:45	15:00	01:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	30:00
w tym suma godzin zajęć	22:30
w tym suma godzin walidacji	01:15
w tym suma przerw	06:15
Suma godzin dydaktycznych bez przerw	31:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 600,00 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	3 600,00 PLN
Koszt osobogodziny brutto	120,00 PLN
Koszt osobogodziny netto	120,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	30:00

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, certyfikaty inżyniera MikroTik: MTCSE, 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 dostępne na platformie edukacyjnej z zakresu administrowania sieciami komputerowymi.

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.

Wymagany egzamin dostępny w formie osobnej usługi o numerze 2026/06/17/134180/3631961. (opublikowanej na BUR).

Informacje dodatkowe

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

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)

EGZAMIN WYMAGANY: „Inżynier bezpieczeństwa sieci MikroTik MTCSE”.

Egzamin dostępny pod nr usługi 2026/06/17/134180/3631961 na BUR.

Warunki techniczne

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

Teams lub poprzez przeglądarkę internetowa 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 aplikacje 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