

The MicroTik logo is displayed in white. It features a stylized white arc above the letter 'i' in 'Mikro', and the word 'Tik' is in a bold, italicized sans-serif font.

*Mikro***Tik**

The text 'MTCSE' is rendered in a large, bold, yellow sans-serif font, centered on the page.

MTCSE

The text 'MikroTik Certified Security Engineer' is written in a black sans-serif font and is contained within a horizontal yellow rectangular bar.

MikroTik Certified Security Engineer

The text 'Москва, Россия' is written in a white sans-serif font, centered at the bottom of the image.

Москва, Россия



— Курс MTCSE

(Certified Security Engineer)

- для желающих повысить свой уровень знаний в области безопасности сетей.

ЦЕЛЕВАЯ АУДИТОРИЯ:

сетевые инженеры и техники,
желающие развернуть и
поддерживать безопасные сети на
основе устройств MikroTik.

ПРЕДВАРИТЕЛЬНАЯ ПОДГОТОВКА:

Для прохождения инженерного курса (MTCSE) необходимо иметь действующий сертификат MTCNA.

Что будут уметь:

- ✓ Студенты научатся планировать и внедрять соответствующие меры безопасности.
- ✓ Принимать меры по предотвращению сетевых угроз на оборудовании MikroTik.

Что получают:

- ✓ Участники, успешно сдавшие экзамен, получают **международный сертификат MikroTik**, а также в подарок лицензию на RouterOS, фирменный сувенир: кружку админа Mikrotik, маршрутизатор
- ✓ Mikrotik NAP Lite и один час бесплатных телефонных консультаций с тренером независимо от результатов сдачи экзамена.

ПРОГРАММА КУРСА

МОДУЛЬ 1

ВВЕДЕНИЕ /
INTRODUCTION

Атаки, механизмы и сервисы

- Наиболее распространенные угрозы
- Развертывание безопасности RouterOS

Лабораторные работы по модулю

МОДУЛЬ 2

FIREWALL

Поток пакетов, межсетевые экраны

- Stateful firewall
- RAW table
- SYN смягчение последствий наводнения с использованием таблицы RAW
- Конфигурация RouterOS по умолчанию
- Обнаружение атаки на критически важные инфраструктурные сервисы
- Мостовой фильтр
- Дополнительные параметры в фильтре брандмауэра
- ICMP-фильтрация

Лабораторные работы по модулю

МОДУЛЬ 3

OSI LAYER
ATTACKS**MNDP атаки и профилактика**

- DHCP: мошеннические серверы, голодные атаки и предотвращение
- TCP SYN атаки и предотвращение
- UDP-атаки и предотвращение
- ICMP Smurf атаки и профилактика
- FTP, telnet и SSH атаки и перебор
- Обнаружение и предотвращение сканирования портов

Лабораторные работы по модулю

МОДУЛЬ 4

CRYPTOGRAPHY

Введение в криптографию и терминологию

- Методы шифрования
- Алгоритмы - симметричные, асимметричные
- Инфраструктура открытых ключей (PKI)
- Сертификаты

Самозаверяющие сертификаты

Бесплатные действующие сертификаты

Использование сертификатов в RouterOS

Лабораторные работы по модулю

МОДУЛЬ 5

SECURING THE ROUTER

Port knocking

- Безопасные соединения (HTTPS, SSH, WinBox)
- Порты по умолчанию для услуг
- Туннелирование через SSH(PKI)

Лабораторные работы по модулю

МОДУЛЬ 6

БЕЗОПАСНЫЕ ТУННЕЛИ

Введение в IPsec

- L2TP + IPsec
- SSTP с сертификатами

Лабораторные работы по модулю

Стоимость курса

32 000 руб.

- Продолжительность обучения не более 4 (четыре) дня – с 10:00 до 18:00 – дневная группа.
- Продолжительность обучения не более 6 (шесть) дней – Пн. - Пт.: с 18:00 до 22:00
Сб: с 10:00 до 17:00.

ДЛИТЕЛЬНОСТЬ КУРСА:

24 академических часа.

При обучении студент получает -



практики



теории