**Общество с ограниченной ответственностью «КУРСЫ ПО ИТ»**

УТВЕРЖДАЮ
Генеральный директор

Скоромнов Д.А.
«31» августа 2023 г.

# Дополнительная профессиональная программа повышения квалификации «Настройка файрвола и приоритизации трафика на MikroTik»

г. Мытищи

# Оглавление

1. СОКРАЩЕНИЯ ..... 3
2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ..... 3
3. ЦЕЛИ ПРОГРАММЫ ..... 3
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ..... 4
4.1. Общепрофессиональные компетенции ..... 4
4.2. Трудовые функции ..... 4
4.2.1. Администрирование процесса конфигурирования сетевых устройств и программного обеспечения (код B) ..... 4
4.2.2. Администрирование процесса контроля производительности сетевых устройств и программного обеспечения (код C) ..... 6
4.2.3. Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения (код D) ..... 8
5. ВИДЫ АТТЕСТАЦИИ ..... 12
5.1. Текущий контроль ..... 12
5.2. Промежуточная аттестация ..... 12
5.3. Итоговая аттестация ..... 12
6. ФОРМЫ АТТЕСТАЦИИ ..... 13
6.1. Тестирование ..... 13
6.2. Лабораторная работа ..... 13
6.3. Контрольная работа ..... 13
7. КРИТЕРИИ ОЦЕНИВАНИЯ ..... 14
7.1. Оценка результатов тестирования ..... 14
7.2. Оценка лабораторных работ и контрольных работ ..... 14
7.2.1. Оценка в виде шкалы от одного до десяти ..... 14
7.2.2. Оценка в формате зачета ..... 16
7.3. Итоговая оценка за курс ..... 16
8. УЧЕБНЫЙ ПЛАН ..... 17
9. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ..... 20
10. РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ ..... 23
10.1. Модуль 1. Схема прохождения трафика ..... 23
10.1.1. Содержание модуля ..... 23
10.1.2. Оценочные материалы ..... 23
10.2. Модуль 2 Брандмауэр. Раздел 1. Connection Tracker ..... 24
10.2.1. Содержание модуля ..... 24
10.2.2. Оценочные материалы ..... 24

10.3. Модуль 2. Брандмауэр. Раздел 2. Filter ..... 24
10.3.1. Содержание модуля ..... 24
10.3.2. Оценочные материалы ..... 27
10.4. Модуль 2. Брандмауэр. Раздел 3. NAT ..... 29
10.4.1. Содержание модуля ..... 29
10.4.2. Оценочные материалы ..... 29
10.5. Модуль 2. Брандмауэр. Раздел 4. Mangle ..... 30
10.5.1. Содержание модуля ..... 30
10.5.2. Оценочные материалы ..... 31
10.6. Модуль 3. QoS ..... 34
10.6.1. Содержание модуля ..... 34
10.6.2. Оценочные материалы ..... 34
10.7. Итоговая аттестация ..... 35
11. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ ..... 37
11.1. Учебно-методическое обеспечение ..... 37
11.2. Кадровое обеспечение ..... 37
11.3. Самостоятельная работа слушателей ..... 37
11.4. Материально-технические условия ..... 37
11.4.1. Рабочее место слушателя ..... 37
11.4.2. Оборудование для лабораторных работ ..... 38

## 1. СОКРАЩЕНИЯ

В данном документе могут использоваться следующие сокращения:

- КР – контрольная работа.
- ЛР – лабораторная работа.
- ОП – образовательная программа.
- ОПК – общепрофессиональная компетенция.
- СР – самостоятельная работа.

## 2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

**Наименование программы:** Настройка файрвола и приоритизации трафика.

**Срок обучения:** 13 учебных недель.

Одна учебная неделя состоит из пяти дней, которые считаются рабочими по производственному календарю РФ. Границы учебной недели могут не совпадать с границами календарной недели.

**Трудоемкость:** 150 академических часов (1 ак. ч. = 45 минут).

**Форма обучения:** заочная, с применением электронного обучения и дистанционных образовательных технологий.

**Выдаваемый документ:** лица, освоившие программу и успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

**Требования к гражданству:** граждане Российской Федерации и иностранные граждане.

**Требования к опыту работы:** не менее полугода администрирования устройств MikroTik.

**Требования к образованию:** граждане, имеющие оконченное высшее или среднее профессиональное образование, а также получающие высшее или среднее профессиональное образование.

## 3. ЦЕЛИ ПРОГРАММЫ

Цель реализации дополнительной профессиональной программы повышения квалификации «Настройка и приоритизации трафика» – это совершенствование имеющейся и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации в пределах профессионального стандарта «Специалист по администрированию сетевых устройств информационно-коммуникационных систем» (06.027).

В том числе целью программы является подготовка сетевых администраторов для работы со следующим функционалом операционной системой MikroTik RouterOS:

- все разделы IP Firewall (Filter, NAT, Mangle, RAW, Service Ports, Connections, Address Lists и L7 Protocols);
- приоритизация трафика с помощью разных видов очередей (Simple Queue, Interface Queue, Queue Tree)

Так же целью программы является изучение схемы прохождения трафика на устройствах под управлением операционной системы MikroTik RouterOS.

## 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

### 4.1. Общепрофессиональные компетенции

В результате освоения ОП слушатель должен обладать следующими общепрофессиональным компетенциями (ОПК) в соответствии с ФГОС ВО бакалавриата по направлению подготовки «Информатика и вычислительная техника» (09.03.01):

- ОПК-1. Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;
- ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;
- ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
- ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;
- ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем;
- ОПК-6. Способен разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием;
- ОПК-7. Способен участвовать в настройке и наладке программно-аппаратных комплексов;
- ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения;
- ОПК-9. Способен осваивать методики использования программных средств для решения практических задач.

### 4.2. Трудовые функции

В результате освоения ОП совершенствуется выполнение части трудовых функций, приведенных в профессиональном стандарте «Специалист по администрированию сетевых устройств информационно-коммуникационных систем» (06.027).

#### 4.2.1. Администрирование процесса конфигурирования сетевых устройств и программного обеспечения (код B)

##### 4.2.1.1. Настройка параметров сетевых устройств и программного обеспечения согласно технологической политике организации (код B/01.5)

**Трудовые действия**

Разработка стандарта задания параметров для каждого вида администрируемых коммуникационных устройств сети

Разработка стандарта задания параметров для каждого вида администрируемых серверов

Разработка стандарта задания параметров для каждого вида администрируемых операционных систем, применяемых в администрируемой сети

Согласование технологических стандартов организации, которой принадлежит конфигурируемая сеть

Конфигурирование параметров администрируемых сетевых устройств и программного обеспечения согласно утвержденным технологическим стандартам организации

Документирование параметров администрируемых сетевых устройств и программного обеспечения согласно утвержденным технологическим стандартам организации

**Умения**

Использовать отраслевые стандарты при настройке параметров администрируемых сетевых устройств и программного обеспечения

Учитывать и отражать в конфигурации сетевых устройств технологические стандарты организации

Учитывать и отражать в конфигурации сетевых устройств стандарты безопасности

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

**Знания**

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Способы коммуникации процессов операционных систем

Модель ISO для управления сетевым трафиком

Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Основы делопроизводства

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

#### 4.2.1.2. Оценка эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа (B/03.5)

**Трудовые действия**

Анализ производительности администрируемой сети с применением специализированного оборудования и программного обеспечения

Создание профайла (списков) параметров организации, влияющих на защиту от несанкционированного доступа

Проверка правильности используемой политики безопасности

Подготовка отчетов для анализа слабых мест в конфигурации системы безопасности

**Умения**

Применять специальные процедуры управления правами доступа пользователей

Работать с официальными сайтами организаций - разработчиков компонентов администрируемой сети

Работать с официальными рассылками изменений к компонентам администрируемой сети

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

**Знания**

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Модель ISO для управления сетевым трафиком

Модели IEEE

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Федеральные и отраслевые требования по защите сети от несанкционированного доступа

Технологические требования организации, которой принадлежит администрируемая сеть, по защите сети от несанкционированного доступа

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

### 4.2.2. Администрирование процесса контроля производительности сетевых устройств и программного обеспечения (код C)

#### 4.2.2.1. Оценка производительности сетевых устройств и программного обеспечения (код C/01.6)

**Трудовые действия**

Оценка производительности критических приложений, наиболее сильно влияющих на производительность сетевых устройств и программного обеспечения в целом

Планирование требуемой производительности администрируемой сети

Фиксирование оценки готовности системы в специальном документе

**Умения**

Выяснять приемлемые для пользователей параметры работы сети в условиях нормальной обычной работы (базовые параметры)

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

Использовать современные методы контроля производительности инфокоммуникационных систем

**Знания**

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Устройство и принцип работы кабельных и сетевых анализаторов

Средства глубокого анализа сети

Метрики производительности администрируемой сети

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Модель OSI/ISO

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

#### 4.2.2.2. Управление средствами тарификации сетевых ресурсов (C/03.6)

**Трудовые действия**

Использование утилит операционных систем для тарификации сетевых ресурсов

Установка дополнительных программных продуктов для тарификации сетевых ресурсов

Параметризация дополнительных программных продуктов для тарификации сетевых ресурсов

**Умения**

Конфигурировать операционные системы сетевых устройств администрируемой сети

Работать с контрольно-измерительными аппаратными и программными средствами

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

**Знания**

Отчеты управляющей системы

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Модель ISO для управления сетевым трафиком

Модели IEEE

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

### 4.2.3. Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения (код D)

#### 4.2.3.1. Определение параметров безопасности и защиты программного обеспечения сетевых устройств (код D/01.6)

**Трудовые действия**

Планирование защиты приложений от несанкционированного доступа

Оценка безопасности и защиты приложений от несанкционированного доступа

Планирование защиты операционных систем от несанкционированного доступа

Оценка защиты операционных систем от несанкционированного доступа

**Умения**

Выяснять приемлемые для пользователей параметры работы сети в условиях нормальной (обычной) работы (базовые параметры)

Применять аппаратные средства защиты сетевых устройств от несанкционированного доступа

Применять программные средства защиты сетевых устройств от несанкционированного доступа

Применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

**Знания**

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Классификация операционных систем согласно классам безопасности

Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Модель ISO для управления сетевым трафиком

Модели IEEE

Защищенные протоколы управления

Основные средства криптографии

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

#### 4.2.3.2. Установка специальных средств управления безопасностью администрируемой сети (код D/02.6)

**Трудовые действия**

Параметризация операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа

Установка специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа

Установка межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети

**Умения**

Настраивать параметры современных программно-аппаратных межсетевых экранов

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

Сегментировать элементы администрируемой сети

**Знания**

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Модель ISO для управления сетевым трафиком

Модели IEEE

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

#### 4.2.3.3. Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) (код D/03.6)

**Трудовые действия**

Параметризация операционных систем средств удаленного доступа

Установка дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация

Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)

Документирование настроек средств обеспечения безопасности удаленного

**Умения**

Подключать и настраивать современные межсетевые экраны

Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

Работать с контрольно-измерительными аппаратными и программными средствами

**Знания**

Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети

Инструкции по установке администрируемых сетевых устройств

Инструкции по эксплуатации администрируемых сетевых устройств

Инструкции по установке администрируемого программного обеспечения

Инструкции по эксплуатации администрируемого программного обеспечения

Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем

Модель ISO для управления сетевым трафиком

Модели IEEE

Защищенные протоколы управления

Основные средства криптографии

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

## 5. ВИДЫ АТТЕСТАЦИИ

### 5.1. Текущий контроль

Текущий контроль – это проверка учебных достижений слушателей по отдельным темам или по небольшим группам тем. Использование текущего контроля позволяет выстраивать образовательный процесс максимально эффективным образом для достижения планируемых результатов обучения.

Целями проведения текущего контроля являются:

- определение фактического уровня освоения ОП;
- выявление пробелов в освоении ОП на ранних этапах;
- оценка продвижения в освоении ОП;
- проведение слушателями самооценки.

Текущий контроль осуществляется в следующих формах: тестирование, лабораторные работы, контрольные работы.

### 5.2. Промежуточная аттестация

Промежуточная аттестация – это проверка учебных достижений слушателей по относительно большему блоку тем, чем при текущем контроле.

Основной целью проведения промежуточной аттестации является определение навыков использования совокупности полученных знаний по логически объединенной группе или группам тем.

Промежуточная аттестация осуществляется в следующих формах: лабораторные работы и контрольные работы.

### 5.3. Итоговая аттестация

Итоговая аттестация – финальная проверка учебных достижений слушателей в процессе освоения ОП.

Итоговая аттестация осуществляется в форме лабораторной работы. Результат итоговой аттестации определяется оценкой «зачтено» или «не зачтено».

## 6. ФОРМЫ АТТЕСТАЦИИ

### 6.1. Тестирование

Тестирование – форма проверки знаний, при которой слушатели должны выбрать правильные ответы из списка предоставленных вариантов.

Способ оценки тестирования описан в разделе «Критерии оценивания».

### 6.2. Лабораторная работа

Лабораторная работа – вид практической деятельности, во время которой слушатели должны выполнять определенные действия. Также в процессе выполнения ЛР слушатели анализируют те или иные вопросы, принимают решения и делают выводы.

Целями выполнения ЛР являются:

- отработка практических навыков самостоятельной работы;
- увеличение уровня понимания материала ОП;
- выявление пробелов в освоении ОП;
- проведение слушателями самооценки.

В зависимости от того, какие задания предусматривает та или иная ЛР, она может быть представлена несколькими видами, отличающимися определенными показателями, характеристиками и структурными особенностями:

- **Исследовательская ЛР,** в процессе выполнения которой происходит наблюдение за определенными процессами на протяжении энного количества времени и делаются записи полученных итогов, составляются графики, схемы или рисунки.
- **Обобщающая ЛР,** в процессе выполнения которой происходит практическое закрепление материала, полученного в ходе освоения ОП.
- **Проблемная ЛР,** в процессе выполнения которой происходит нахождение варианта решения проблемы, заданной условиями ЛР. В основе такого вида работ лежат теоретические знания, которые необходимо научиться применять практически, делая выводы.

Для лабораторных работ, которые подразумевают выставление оценки, способ оценивания описан в разделе «Критерии оценивания».

### 6.3. Контрольная работа

Контрольная работа (контрольное задание) – форма проверки знаний, при которой слушатели должны дать письменный ответ на поставленные вопросы.

Целями выполнения КР являются:

- оценка навыков использования знаний, полученных в процессе освоения ОП;
- увеличение уровня понимания материала ОП;
- выявление пробелов в освоении ОП;
- проведение слушателями самооценки.

Способ оценки контрольных работ описан в разделе «Критерии оценивания».

# 7. КРИТЕРИИ ОЦЕНИВАНИЯ

## 7.1. Оценка результатов тестирования

Оценка тестов происходит с точностью до сотых долей. Независимо от количества вопросов в блоке тестов, суммарно за весь блок тестов не может быть начислено более 10 баллов. При разном количестве вопросов в блоке тестов максимальное количество баллов, которые могут быть начислены за каждый отдельный вопрос, будет различаться. Изначально максимальное количество баллов, которые могут быть начислены за каждый отдельный вопрос в блоке тестов, одинаковое. Но в зависимости от сложности вопроса для него может быть использован повышающий или, наоборот, понижающий коэффициент. При наборе 7,5 (семи целых пяти десятых) балла и более тестирование считается успешно пройденным.

Основная масса вопросов относится к одному из следующих видов:

- вопросы, в которых в качестве ответа необходимо указать некое значение;
- вопросы вида «истина или ложь»;
- вопросы с одним правильным ответом;
- вопросы с несколькими правильными ответами;
- вопросы на выбор соответствия.

Первые три категории имеют фиксированное количество баллов за правильный ответ в пределах блока тестов. У вопросов с несколькими правильными ответами и у вопросов на выбор соответствия количество полученных баллов может быть различным. Оно зависит от числа выбранных правильных и неправильных вариантов ответов. При ответе на вопрос любого вида нельзя получить менее 0 баллов.

В вопросах с возможностью множественного выбора правильных ответов должно быть более одного и все ответы не могут быть правильными. Максимальное количество баллов, которые могут быть получены за вопрос, делится на количество правильных ответов. Частное (результат деления) будет являться количеством баллов, которые могут быть получены за отдельный правильный ответ. Максимальное количество баллов, которые могут быть получены за вопрос, делится на количество неправильных ответов. Частное (результат деления) будет являться количеством баллов, которые могут быть сняты за отдельный неправильный ответ. Таким образом, если в вопросе одновременно выбрать все варианты ответов, то получится, что сумма всех начисленных баллов будет равна сумме всех снятых баллов, и в итоге за вопрос будет начислено ноль баллов. Но при этом так же, как и при других видах вопросов, получить менее ноля баллов за вопрос нельзя.

## 7.2. Оценка лабораторных работ и контрольных работ

### 7.2.1. Оценка в виде шкалы от одного до десяти

#### 7.2.1.1. Определения

**Условия задания** – любые условия, которые указаны в задании, в том числе и условия нетехнического характера. Пример условия нетехнического характера: сделайте в ответе нумерованный список.

**Ошибка** (в процессе решения) – ошибочное решение задания. Если в задании требуется найти ошибки в конфигурации и найдены не все ошибки, то это не считается ошибкой (в процессе решения), а считается неполным решением задания. Ошибкой (в процессе

решения) считается указание слушателем на ошибку в конфигурации, которая таковой не является.

**Подсказка** – помощь куратора в поиске ошибки или в поиске того, что было выполнено не полностью, без прямого указания на ошибку или на то, что было сделано не полностью.

#### 7.2.1.2. Оценка

Оценка происходит с точностью до единицы.

**10 баллов** (5, отлично) – слушатель самостоятельно, с первой попытки, полностью и без ошибок выполнил контрольное задание.

**9 баллов** (5, отлично) – слушатель самостоятельно выполнил контрольное задание. Полностью задание было выполнено со второй или третьей попытки. Куратор не оказывал помощи в поиске того, что не было сделано, а только подсказывал, что имеется такой факт. При выполнении задания не было допущено ни одной ошибки.

**8 баллов** (4, хорошо) – слушатель самостоятельно выполнил контрольное задание. При выполнении задания не было допущено ни одной ошибки. Условия получения оценки:

- Полностью задание было выполнено с четвертой или пятой попытки. Куратор не оказывал помощи в поиске того, что не было сделано, а только подсказывал, что имеется такой факт.
- Полностью задание было выполнено с количеством попыток от двух до пяти включительно. Для выполнения задания потребовалась одна подсказка без указания на то, что не сделано или сделано некорректно.

**7 баллов** (4, хорошо) – слушатель самостоятельно выполнил контрольное задание. Условия получения оценки:

- Полностью задание было выполнено с количеством попыток от двух до пяти включительно. Для выполнения задания потребовались две или три подсказки без прямого указания на то, что не сделано или сделано некорректно. При выполнении задания не было допущено ни одной ошибки.
- Полностью задание было выполнено с количеством попыток от двух до пяти включительно. Было допущено не более двух ошибок, которые слушатель нашел самостоятельно после указания на факт наличия ошибки.
- Полностью задание было выполнено с количеством попыток от двух до пяти включительно. Была допущена одна ошибка, которую слушатель не смог найти самостоятельно.

**6 и 5 баллов** (3, удовлетворительно) – слушатель самостоятельно выполнил только часть контрольного задания и (или) в решении имелись ошибки, которые слушатель не смог обнаружить самостоятельно. Конкретная оценка выставляется на усмотрение проверяющего.

**4, 3, 2 и 1 балл** (2, неудовлетворительно) – слушатель не смог выполнить контрольное задание. Конкретная оценка выставляется на усмотрение проверяющего.

### 7.2.2. Оценка в формате зачета

| Оценка | Требования к знаниям |
|---|---|
| **Зачтено** | Усвоил теоретический и практический материал.<br>Логично и грамотно излагает материал.<br>Связывает теоретические знания и практические навыки.<br>Делает корректные выводы и обобщения. |
| **Не зачтено** | Не усвоил значительную часть теоретического и практического материала ОП.<br>Допускает существенные ошибки и неточности.<br>Испытывает трудности в связывании теоретических знаний и практических навыков.<br>Испытывает трудности в аргументации. |

### 7.3. Итоговая оценка за курс

Итоговая оценка за курс высчитывается с помощью процентного соотношения всех набранных баллов к максимально возможному количеству баллов, которые суммарно можно получить за весь курс. Далее на основе процентной оценки определяется результат за весь курс. Изначально все элементы оценки полученных знаний равны друг другу по значимости, но в зависимости от сложности для отдельных элементов может быть использован повышающий или, наоборот, понижающий коэффициент.

Для удобства слушателей результаты элементов оценки также переводятся в классическую школьную пятибалльную шкалу (от 2 до 5, где 2 – наихудшая оценка, а 5 – наилучшая оценка) и в европейскую шкалу (от F до A, где F – наихудшая оценка, а A – наилучшая оценка).

| Процентная шкала | Классическая шкала | Европейская шкала |
|---|---|---|
| 87–100 % | 5 (отлично) | B+, A-, A |
| 73–86,99 % | 4 (хорошо) | C, C+, B-, B |
| 60–72,99 % | 3 (удовлетворительно) | D, D+, C- |
| 0–59,99 % | 2 (неудовлетворительно) | F |

## 8. УЧЕБНЫЙ ПЛАН

| Наименование (модулей, тем) | Всего (ак. ч.) | Виды учебной работы (ак. ч.) | | | | | Контроль (шт.) | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Лекции | ЛР | КР | Тесты | СР | ЛР | КР | Тесты |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **Модуль 1. Схема прохождения трафика** | | | | | | | | | |
| Схемы прохождения трафика | 0,6 | 0,1 | | | 0,5 | 0,0 | | | 1 |
| Простейшая схема прохождения трафика | 0,3 | 0,2 | | | | 0,1 | | | |
| Содержимое цепочек | 0,2 | 0,1 | | | | 0,1 | | | |
| Простая схема прохождения трафика | 0,2 | 0,1 | | | | 0,1 | | | |
| Ошибки | 0,5 | 0,4 | | | | 0,1 | | | |
| Выбор интерфейса | 0,2 | 0,1 | | | | 0,1 | | | |
| **Всего по модулю** | **2,0** | **1,0** | **0,0** | **0,0** | **0,5** | **0,5** | **0** | **0** | **1** |
| **Модуль 2. Файрвол. Раздел 1. Connection Tracker** | | | | | | | | | |
| Назначение Connection Tracker | 2,0 | 0,3 | 0,5 | | 0,5 | 0,7 | 2 | | 1 |
| **Всего по модулю** | **2,0** | **0,3** | **0,5** | **0,0** | **0,5** | **0,7** | **2** | **0** | **1** |
| **Модуль 2. Брандмауэр. Раздел 2. Filter** | | | | | | | | | |
| Принцип действия брандмауэра | 5,9 | 0,5 | | | 3 | 2,4 | | | 1 |
| Условия со вкладок General, Action и Advanced | 2,7 | 1,1 | 0,5 | | | 1,1 | | | |
| Брандмауэр в реальной жизни | 1,8 | 0,6 | 0,5 | | | 0,7 | 1 | | |
| Гостевая сеть | 1,0 | 0,1 | 0,5 | | | 0,4 | 1 | | |
| Bridge Filter | 0,1 | 0,1 | | | | 0,0 | | | |
| DMZ | 1,0 | 0,1 | 0,5 | | | 0,4 | 1 | | |
| Список адресов | 3,9 | 0,3 | 2 | | | 1,6 | 1 | | |
| Блокировка при попытке подбора пароля SSH | 5,0 | | 5 | | | 0,0 | 1 | | |
| Доступ к SSH после перебора портов (1 и 2 способ) | 20,0 | | 20 | | | 0,0 | 2 | | |
| Основы сетевой и информационной безопасности | 1,1 | 0,7 | | | | 0,4 | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Вкладка Extra | 1,1 | 0,7 | | | | 0,4 | | | |
| Защита от DoS-атак с помощью Connection Limit | 0,5 | 0,3 | | | | 0,2 | | | |
| Дополнительная защита от SYN-flood атаки | 0,1 | 0,1 | | | | 0,0 | | | |
| Пользовательские цепочки | 1,1 | 0,2 | 0,5 | | | 0,4 | 1 | | |
| Защита от DoS-атак с помощью Destination Limit | 1,0 | 0,1 | 0,5 | | | 0,4 | 1 | | |
| Защита от сканирования портов | 0,6 | 0,4 | | | | 0,2 | | | |
| Доступ к SSH после перебора портов (3 способ) | 1,0 | | 1 | | | 0,0 | 1 | | |
| RAW Filter | 0,1 | 0,1 | | | | 0,0 | | | |
| Fast Track | 0,3 | 0,2 | | | | 0,1 | | | |
| L7-фильтр | 0,1 | 0,1 | | | | 0,0 | | | |
| Блокировка сайтов, торрентов и Tor | 1,3 | 0,3 | 0,5 | | | 0,5 | 1 | | |
| Поиск ошибок в брандмауэре | 0,5 | 0,3 | | | | 0,2 | | | |
| Прочее | 3,3 | 0,2 | 0,5 | | | 2,6 | 1 | | |
| Промежуточная аттестация | 1,5 | | 0,5 | 1 | | | 1 | 1 | |
| **Всего по модулю** | **55,0** | **6,5** | **32,5** | **1,0** | **3,0** | **12,0** | **13** | **1** | **1** |
| **Модуль 2. Файрвол. Раздел 3. NAT** | | | | | | | | | |
| Основы NAT | 2,5 | 0,4 | 0,5 | | 1 | 0,6 | 1 | | 1 |
| Destination NAT | 2,2 | 0,5 | 0,5 | 0,5 | | 0,7 | 1 | 1 | |
| Source NAT | 3,9 | 0,3 | 2 | | | 1,6 | 1 | | |
| Netmap | 5,1 | 0,1 | 5 | | | 0,0 | 1 | | |
| Нюансы NAT | 0,3 | 0,2 | | | | 0,1 | | | |
| Нестандартные ситуации использования NAT | 20,0 | | 20 | | | 0,0 | 2 | | |
| **Всего по модулю** | **34,0** | **1,5** | **28,0** | **0,5** | **1,0** | **3,0** | **6** | **1** | **1** |
| **Модуль 2. Файрвол. Раздел 4. Mangle** | | | | | | | | | |
| Основы Mangle | 0,7 | 0,1 | | | 0,5 | 0,1 | | | 1 |
| Маркировка трафика | 1,3 | 0,3 | 0,5 | | | 0,5 | 2 | | |
| Выбор цепочки | 0,2 | 0,1 | | | | 0,1 | | | |
| Порядок обработки | 3,4 | 0,4 | 1 | 1 | | 1,0 | 1 | 1 | |
| Лучшие практики по маркировке трафика | 2,4 | 0,4 | 1 | | | 1,0 | 1 | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Маркировка трафика для IP-телефонии | 3,5 | 0,1 | 1 | 1 | | 1,4 | 1 | 1 | |
| Маркировка маршрутов | 1,0 | 0,1 | 0,5 | | | 0,4 | 1 | | |
| Балансировка нагрузки между двумя интернет-каналами | 0,5 | 0,3 | | | | 0,2 | | | |
| Промежуточная аттестация | 6,0 | | 6 | | | | 3 | | |
| **Всего по модулю** | **19,0** | **1,8** | **10,0** | **2,0** | **0,5** | **4,7** | **9** | **2** | **1** |
| **Модуль 3. Приоритизация трафика** | | | | | | | | | |
| Simple Queue | 2,5 | 0,7 | 0,5 | | 0,5 | 0,8 | 1 | | 1 |
| Queue Tree | 1,7 | 0,3 | 0,5 | | | 0,9 | 1 | | |
| Режим Burst | 0,1 | 0,1 | | | | 0,0 | | | |
| Приоритизация трафика | 15,1 | 1,3 | 6 | 6 | | 1,8 | 1 | 3 | |
| Типы очередей | 2,0 | 0,7 | 0,5 | | | 0,8 | 1 | | |
| Прочее | 0,6 | 0,3 | | | | 0,3 | | | |
| Промежуточная аттестация | 6,0 | | 6 | | | | 1 | | |
| **Всего по модулю** | **28,0** | **3,4** | **13,5** | **6,0** | **0,5** | **4,6** | **5** | **3** | **1** |
| **Итоговая аттестация** | | | | | | | | | |
| Итоговая аттестация | 10,0 | | 10 | | | | 1 | | |
| **Всего по аттестации** | **10,0** | **0,0** | **10,0** | **0,0** | **0,0** | **0,0** | **1** | **0** | **0** |
| **Всего по образовательной программе** | **150,0** | **14,5** | **94,5** | **9,5** | **6,0** | **25,5** | **36** | **7** | **6** |

Обучение может быть организовано по индивидуальному учебному плану с учетом особенностей и образовательных потребностей конкретного слушателя.

## 9. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

| Наименование (модулей, тем) | Всего (ак. ч.) | Неделя | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| **Модуль 1. Схема прохождения трафика** | | | | | | | | | | | | | | |
| Схемы прохождения трафика | 0,6 | 0,6 | | | | | | | | | | | | |
| Простейшая схема прохождения трафика | 0,3 | 0,3 | | | | | | | | | | | | |
| Содержимое цепочек | 0,2 | 0,2 | | | | | | | | | | | | |
| Простая схема прохождения трафика | 0,2 | 0,2 | | | | | | | | | | | | |
| Ошибки | 0,5 | 0,5 | | | | | | | | | | | | |
| Выбор интерфейса | 0,2 | 0,2 | | | | | | | | | | | | |
| **Всего по модулю** | **2,0** | **2,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** |
| **Модуль 2. Файрвол. Раздел 1. Connection Tracker** | | | | | | | | | | | | | | |
| Назначение Connection Tracker | 2,0 | 2,0 | | | | | | | | | | | | |
| **Всего по модулю** | **2,0** | **2,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** |
| **Модуль 2. Брандмауэр. Раздел 2. Filter** | | | | | | | | | | | | | | |
| Принцип действия брандмауэра | 5,9 | 5,9 | | | | | | | | | | | | |
| Условия со вкладок General, Action и Advanced | 2,7 | 1,7 | 1,0 | | | | | | | | | | | |
| Брандмауэр в реальной жизни | 1,8 | | 1,8 | | | | | | | | | | | |
| Гостевая сеть | 1,0 | | 1,0 | | | | | | | | | | | |
| Bridge Filter | 0,1 | | 0,1 | | | | | | | | | | | |
| DMZ | 1,0 | | 1,0 | | | | | | | | | | | |
| Список адресов | 3,9 | | 3,9 | | | | | | | | | | | |
| Блокировка при попытке подбора пароля SSH | 5,0 | | 2,7 | 2,3 | | | | | | | | | | |
| Доступ к SSH после перебора портов (1 и 2 способ) | 20,0 | | | 9 | 11 | | | | | | | | | |
| Основы сетевой и информационной безопасности | 1,1 | | | | | 1,1 | | | | | | | | |
| Вкладка Extra | 1,1 | | | | | 1,1 | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Защита от DoS-атак с помощью Connection Limit | 0,5 | | | | | 0,5 | | | | | | | | |
| Дополнительная защита от SYN-flood атаки | 0,1 | | | | | 0,1 | | | | | | | | |
| Пользовательские цепочки | 1,1 | | | | | 1,1 | | | | | | | | |
| Защита от DoS-атак с помощью Destination Limit | 1,0 | | | | | 1,0 | | | | | | | | |
| Защита от сканирования портов | 0,6 | | | | | 0,6 | | | | | | | | |
| Доступ к SSH после перебора портов (3 способ) | 1,0 | | | | | 1,0 | | | | | | | | |
| RAW Filter | 0,1 | | | | | 0,1 | | | | | | | | |
| Fast Track | 0,3 | | | | | 0,3 | | | | | | | | |
| L7-фильтр | 0,1 | | | | | 0,1 | | | | | | | | |
| Блокировка сайтов, торрентов и Tor | 1,3 | | | | | 1,3 | | | | | | | | |
| Поиск ошибок в брандмауэре | 0,5 | | | | | 0,5 | | | | | | | | |
| Прочее | 3,3 | | | | | 3,3 | | | | | | | | |
| Промежуточная аттестация | 1,5 | | | | | | 1,5 | | | | | | | |
| **Всего по модулю** | **55,0** | **7,6** | **11,5** | **11,3** | **11,0** | **12,1** | **1,5** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** |
| **Модуль 2. Файрвол. Раздел 3. NAT** | | | | | | | | | | | | | | |
| Основы NAT | 2,5 | | | | | | 2,5 | | | | | | | |
| Destination NAT | 2,2 | | | | | | 2,2 | | | | | | | |
| Source NAT | 3,9 | | | | | | 3,9 | | | | | | | |
| Netmap | 5,1 | | | | | | 1,5 | 3,6 | | | | | | |
| Нюансы NAT | 0,3 | | | | | | | 0,3 | | | | | | |
| Нестандартные ситуации использования NAT | 20,0 | | | | | | | 8 | 12 | | | | | |
| **Всего по модулю** | **34,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **10,1** | **11,9** | **12,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** |
| **Модуль 2. Файрвол. Раздел 4. Mangle** | | | | | | | | | | | | | | |
| Основы Mangle | 0,7 | | | | | | | | | 0,7 | | | | |
| Маркировка трафика | 1,3 | | | | | | | | | 1,3 | | | | |
| Выбор цепочки | 0,2 | | | | | | | | | 0,2 | | | | |
| Порядок обработки | 3,4 | | | | | | | | | 3,4 | | | | |
| Лучшие практики по маркировке трафика | 2,4 | | | | | | | | | 2,4 | | | | |
| Маркировка трафика для IP-телефонии | 3,5 | | | | | | | | | 3,5 | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Маркировка маршрутов | 1,0 | | | | | | | | | | 1,0 | | | |
| Балансировка нагрузки между двумя интернет-каналами | 0,5 | | | | | | | | | | 0,5 | | | |
| Промежуточная аттестация | 6,0 | | | | | | | | | | 6,0 | | | |
| **Всего по модулю** | **19,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **11,5** | **7,5** | **0,0** | **0,0** | **0,0** |
| **Модуль 3. Приоритизация трафика** | | | | | | | | | | | | | | |
| Simple Queue | 2,5 | | | | | | | | | | 2,5 | | | |
| Queue Tree | 1,7 | | | | | | | | | | 1,7 | | | |
| Режим Burst | 0,1 | | | | | | | | | | | 0,1 | | |
| Приоритизация трафика | 15,1 | | | | | | | | | | | 11,7 | 3,4 | |
| Типы очередей | 2,0 | | | | | | | | | | | | 2,0 | |
| Прочее | 0,6 | | | | | | | | | | | | 0,6 | |
| Промежуточная аттестация | 6,0 | | | | | | | | | | | | 6,0 | |
| **Всего по модулю** | **28,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **4,2** | **11,8** | **12,0** | **0,0** |
| **Итоговая аттестация** | | | | | | | | | | | | | | |
| Итоговая аттестация | 10,0 | | | | | | | | | | | | | 10 |
| **Всего по аттестации** | **10,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **0,0** | **10,0** |
| **Всего по образовательной программе** | **150,0** | **11,6** | **11,5** | **11,3** | **11,0** | **12,1** | **11,6** | **11,9** | **12,0** | **11,5** | **11,7** | **11,8** | **12,0** | **10,0** |

# 10. РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ

## 10.1. Модуль 1. Схема прохождения трафика

### 10.1.1. Содержание модуля

#### 10.1.1.1. Тема № 1. Схемы прохождения трафика

В рамках темы должны быть изучены существующие схемы прохождения трафика (официальные и неофициальные) и их назначение.

#### 10.1.1.2. Тема № 2. Простейшая схема прохождения трафика

В рамках темы должна быть изучена простейшая схема прохождения пакетов.

#### 10.1.1.3. Тема № 3. Содержимое цепочек

В рамках темы должно быть произведено знакомство с логическими элементами, которые располагаются в цепочках Prerouting, Input, Output, Forward и Postrouting.

#### 10.1.1.4. Тема № 4. Простая схема прохождения трафика

В рамках темы должна быть изучена простая схема прохождения трафика.

#### 10.1.1.5. Тема № 5. Ошибки

В рамках темы должны быть изучены распространенные ошибки, которые встречаются в ситуациях, когда сетевой администратор для создания конфигураций не использует схему прохождения трафика.

#### 10.1.1.6. Тема № 6. Выбор интерфейса

В рамках темы должны быть изучены принципы, на основе которых необходимо делать выбор интерфейса в различных конфигурациях.

### 10.1.2. Оценочные материалы

Ниже приведены примеры оценочных материалов, которые используются в модуле № 1.

#### 10.1.2.1. Тестирование

Ниже приведены примеры тестовых вопросов, которые используются в модуле:

- В какой из цепочек отсутствует возможность маркировки пакета?
- В каком объекте и в какой из цепочек происходит отслеживание соединений?
- Какие цепочки используются, если запустить ping с маршрутизатора до 8.8.8.8?

#### 10.1.2.2. Лабораторные работы

Лабораторные работы в модуле отсутствуют.

#### 10.1.2.3. Контрольные работы

Контрольные работы в модуле отсутствуют.

### 10.2. Модуль 2 Брандмауэр. Раздел 1. Connection Tracker

#### 10.2.1. Содержание модуля

#### 10.2.1.1. Тема № 1. Назначение Connection Tracker

В рамках темы должно быть изучено назначение службы отслеживания соединений (Connection Tracker) и ее настройки.

#### 10.2.2. Оценочные материалы

Ниже приведены примеры оценочных материалов, которые используются в модуле № 2.1.

#### 10.2.2.1. Тестирование

Ниже приведены примеры тестовых вопросов, которые используются в модуле:

- Как называется соединение, которое является обязательным до создания related-соединения?
- Есть ли способы миновать Connection Tracker? Если есть, то что требуется для их реализации?

#### 10.2.2.2. Лабораторные работы

**Лабораторная работа № 2.1.1. Первоначальная настройка маршрутизатора**

Целью лабораторной работы является создание сетевой топологии, которая будет использоваться в дальнейшем.

**Лабораторная работа № 2.1.2. Connection Tracker**

В рамках лабораторной работы должны быть закреплены практические навыки работы с Connection Tracker.

#### 10.2.2.3. Контрольные работы

Контрольные работы в модуле отсутствуют.

### 10.3. Модуль 2. Брандмауэр. Раздел 2. Filter

#### 10.3.1. Содержание модуля

#### 10.3.1.1. Тема № 1. Принцип действия брандмауэра

В рамках темы должны быть изучены следующие подтемы:

- что нельзя сделать с помощью брандмауэра MikroTik RouterOS;
- принцип действия брандмауэра MikroTik RouterOS.

#### 10.3.1.2. Тема № 2. Условия со вкладок General, Action и Advanced

В рамках темы должны быть изучены условия, доступные через графический интерфейс в настройках правил IP Firewall Filter на вкладках General, Action и Advanced.

#### 10.3.1.3. Тема № 3. Брандмауэр в реальной жизни

В рамках темы должна быть изучена базовая настройка брандмауэра MikroTik RouterOS, которая может быть использована в реальных условиях. Также должна быть изучена взаимосвязь IP Firewall Filter и Connection Tracker.

#### 10.3.1.4. Тема № 4. Гостевая сеть

В рамках темы должны быть изучены назначение и настройка гостевой сети.

#### 10.3.1.5. Тема № 5. Bridge Filter

В рамках темы должно быть произведено знакомство с возможностями Bridge Filter.

#### 10.3.1.6. Тема № 6. DMZ

В рамках темы должны быть изучены назначение и настройка демилитаризованной зоны (DMZ).

#### 10.3.1.7. Тема № 7. Список адресов

В рамках темы должны быть изучены возможности адресных списков.

#### 10.3.1.8. Тема № 8. Блокировка при попытке подбора пароля SSH

В рамках темы должны быть изучены настройки, необходимые для выполнения блокировки IP-адресов, с которых будут обнаружены многократные попытки подключения по SSH.

#### 10.3.1.9. Тема № 9. Доступ к SSH после перебора портов (1-й и 2-й способ)

В рамках темы должны быть изучены настройки, необходимые для того, чтобы разрешить подключение к устройству MikroTik с помощью протокола SSH, после того как будут произведены попытки подключения по заранее заданной комбинации портов. Должны быть изучены два способа: когда порядок указания портов играет роль и когда порядок указания портов не играет роли.

#### 10.3.1.10. Тема № 10. Основы сетевой и информационной безопасности

В рамках темы должны быть изучены основы сетевой и информационной безопасности и распространенные сетевые атаки.

#### 10.3.1.11. Тема № 11. Вкладка Extra

В рамках темы должны быть изучены условия, доступные через графический интерфейс в настройках правил IP Firewall Filter на вкладке Extra.

#### 10.3.1.12. Тема № 12. Защита от DoS-атак с помощью Connection Limit

В рамках темы должна быть изучена защита от DoS-атак с помощью условия Connection Limit.

#### 10.3.1.13. Тема № 13. Дополнительная защита от SYN-flood-атаки

В рамках темы должны быть изучены дополнительные возможности по защите от SYN-flood-атак.

#### 10.3.1.14. Тема № 14. Пользовательские цепочки

В рамках темы должны быть изучены пользовательские цепочки.

#### 10.3.1.15. Тема № 15. Защита от DoS-атак с помощью Destination Limit

В рамках темы должна быть изучена защита от DoS-атак с помощью условия Destination Limit.

#### 10.3.1.16. Тема № 16. Защита от сканирования портов

В рамках темы должны быть изучены настройки, которые позволят обеспечить защиту от сканирования портов, а также сервисы Whois и IPLookup.

#### 10.3.1.17. Тема № 17. Доступ к SSH после перебора портов (3-й способ)

В рамках темы должны быть изучены настройки, необходимые для того, чтобы разрешить подключение к устройству MikroTik с помощью протокола SSH, после того как будут произведены попытки подключения по заранее заданной комбинации портов. Должен быть изучен самый простой способ, при котором порядок указания портов не играет роли.

#### 10.3.1.18. Тема № 18. RAW Filter

В рамках темы должны быть изучены возможности RAW Filter и его отличие от IP Firewall Filter.

#### 10.3.1.19. Тема № 19. Fast Track

В рамках темы должна быть изучена технология Fast Track.

#### 10.3.1.20. Тема № 20. L7-фильтр

В рамках темы должны быть изучены возможности L7-фильтра.

#### 10.3.1.21. Тема № 21. Блокировка сайтов, торрентов и Tor

В рамках темы должны быть изучены возможности по блокировке сайтов, торрентов и браузера Tor.

#### 10.3.1.22. Тема № 22. Поиск ошибок в брандмауэре

В рамках темы должны быть изучены способы поиска ошибок в настройках брандмауэра.

#### 10.3.1.23. Тема № 23. Прочее

В рамках темы должны быть изучены прочие нюансы использования брандмауэра MikroTik RouterOS, о которых не говорилось ни в одной из предыдущих тем.

### 10.3.2. Оценочные материалы

Ниже приведены примеры оценочных материалов, которые используются в модуле № 2.2.

#### 10.3.2.1. Тестирование

Ниже приведены примеры тестовых вопросов, которые используются в модуле:

- Какая информация содержится в сокете?
- В каких цепочках нет IP Firewall Filter?
- Какой тип брандмауэра является более безопасным?

#### 10.3.2.2. Лабораторные работы

**Лабораторная работа № 2.2.1. Составление правил**

В рамках лабораторной работы должны быть закреплены практические навыки создания правил IP Firewall Filter.

**Лабораторная работа № 2.2.2. Брандмауэр в реальной жизни**

В рамках лабораторной работы должны быть закреплены практические навыки настройки правил, которые в совокупности будут представлять собой брандмауэр, который может быть использован в реальных условиях.

**Лабораторная работа № 2.2.3. Гостевая сеть**

В рамках лабораторной работы должны быть закреплены практические навыки настройки гостевой сети.

**Лабораторная работа № 2.2.4. DMZ**

В рамках лабораторной работы должны быть закреплены практические навыки настройки демилитаризованной зоны.

**Лабораторная работа № 2.2.5. Блокировка при попытке подбора пароля SSH**

В рамках лабораторной работы должны быть закреплены практические навыки блокировки IP-адресов, с которых будут обнаружены многократные попытки подключения по SSH.

**Лабораторная работа № 2.2.6. Доступ по SSH после перебора портов – 1**

В рамках лабораторной работы должны быть закреплены практические навыки настройки предоставления возможности подключения к устройству MikroTik с помощью протокола SSH, после того как будут произведены попытки подключения по заранее заданной комбинации портов в ситуации, когда порядок перебора портов играет роль.

**Лабораторная работа № 2.2.7. Доступ по SSH после перебора портов – 2**

В рамках лабораторной работы должны быть закреплены практические навыки настройки предоставления возможности подключения к устройству MikroTik с помощью протокола SSH, после того как будут произведены попытки подключения по заранее заданной комбинации портов в ситуации, когда порядок перебора портов не играет роли.

**Лабораторная работа № 2.2.8. Пользовательские цепочки**

В рамках лабораторной работы должны быть закреплены практические навыки настройки пользовательских цепочек.

**Лабораторная работа № 2.2.9. Защита от DoS-атак с помощью Destination Limit**

В рамках лабораторной работы должны быть закреплены практические навыки настройки защиты от DoS-атак с помощью условия Destination Limit.

**Лабораторная работа № 2.2.10. Доступ по SSH после перебора портов – 3**

В рамках лабораторной работы должны быть закреплены практические навыки настройки предоставления возможности подключения к устройству MikroTik с помощью протокола SSH, после того как будут произведены попытки подключения по заранее заданной комбинации портов в ситуации, когда порядок перебора портов не играет роли. Отличие от предыдущей аналогичной лабораторной работы заключается в том, что данный способ является намного более простым.

**Лабораторная работа № 2.2.11. Блокировка сайтов**

В рамках лабораторной работы должны быть закреплены практические навыки настройки блокировки доступа к интернет-сайтам различными способами.

**Лабораторная работа № 2.2.12. Дополнительные способы защиты**

В рамках лабораторной работы должны быть закреплены практические навыки настройки дополнительных способов защиты.

**Лабораторная работа № 2.2.13. Финальная**

Лабораторная работа используется для промежуточной аттестации.

В рамках лабораторной работы должны быть закреплены практические навыки анализа взаимосвязанных правил IP Firewall Filter в сложных конфигурациях.

#### 10.3.2.3. Контрольные работы

**Контрольная работа № 2.2.1. Поиск ошибок в настройках IP Firewall Filter**

Контрольная работа используется для промежуточной аттестации.

В рамках контрольной работы должны быть проверены навыки поиска ошибок в настройках IP Firewall Filter.

### 10.4. Модуль 2. Брандмауэр. Раздел 3. NAT

#### 10.4.1. Содержание модуля

##### 10.4.1.1. Тема № 1. Основы NAT

В рамках темы должно быть изучено назначение технологии NAT без привязки к какому-либо вендору.

##### 10.4.1.2. Тема № 2. Destination NAT

В рамках темы должна быть изучена разновидность NAT – Destination NAT. В том числе должна быть изучена самая распространенная ситуация применения Destination NAT – проброс портов.

##### 10.4.1.3. Тема № 3. Source NAT

В рамках темы должна быть изучена разновидность NAT – Source NAT. В том числе должны быть изучены: ошибка при использовании masquerade и настройки, необходимые для подключения по внешнему IP-адресу с одного устройства, находящегося в локальной сети, на другое устройство, находящееся в той же локальной сети (Hairpin NAT).

##### 10.4.1.4. Тема № 4. Netmap

В рамках темы должны быть изучены настройки NAT, с помощью которых можно обеспечить L3-связь между сетями, которые имеют одинаковые адреса.

##### 10.4.1.5. Тема № 5. Нюансы NAT

В рамках темы должны быть изучены различные нюансы использования NAT: NAT helpers, специфика связки NAT, IP и двух и более интернет-каналов.

##### 10.4.1.6. Тема № 6. Нестандартные ситуации использования NAT

В рамках темы должны быть изучены нестандартные ситуации использования NAT.

#### 10.4.2. Оценочные материалы

Ниже приведены примеры оценочных материалов, которые используются в модуле № 2.3.

##### 10.4.2.1. Тестирование

Ниже приведены примеры тестовых вопросов, которые используются в модуле:

- Какой из видов NAT может повлиять на выбор дальнейшей цепочки?
- В каких случаях надо использовать action=masquerade?

##### 10.4.2.2. Лабораторные работы

**Лабораторная работа № 2.3.1. Базовая**

В рамках лабораторной работы должно быть закреплено понимание принципов работы NAT.

**Лабораторная работа № 2.3.2. Destination NAT**

В рамках лабораторной работы должны быть закреплены практические навыки работы с Destination NAT.

**Лабораторная работа № 2.3.3. Source NAT**

В рамках лабораторной работы должны быть закреплены практические навыки работы с Source NAT.

**Лабораторная работа № 2.3.4. Netmap**

В рамках лабораторной работы должны быть закреплены практические навыки настройки правил NAT, с помощью которых можно обеспечить L3-связь между сетями, которые имеют одинаковые адреса сетей.

**Лабораторная работа № 2.3.5. Нестандартное использование NAT № 1**

В рамках лабораторной работы должно быть найдено решение того, как при RDP-подключении на внешний IP-адрес одного маршрутизатора по факту оказаться подключенным к RDP-серверу, который находится за другим маршрутизатором, при условии что между двумя маршрутизаторами есть VPN-соединение.

**Лабораторная работа № 2.3.6. Нестандартное использование NAT № 2**

В рамках лабораторной работы должно быть найдено решение того, как при подключении с одного заданного маршрутизатора на другой маршрутизатор устанавливалось бы VPN-соединение между двумя маршрутизаторами, а при подключении с любого другого устройства на тот же самый порт, на который подключается заданный маршрутизатор, происходил бы проброс порта на сервер за маршрутизатором.

#### 10.4.2.3. Контрольные работы

**Контрольная работа № 2.3.1**

В рамках контрольной работы должны быть проверены навыки поиска ошибок в настройках IP Firewall NAT.

### 10.5. Модуль 2. Брандмауэр. Раздел 4. Mangle

#### 10.5.1. Содержание модуля

#### 10.5.1.1. Тема № 1. Основы Mangle

В рамках темы должны быть изучены назначение и возможные настройки IP Firewall Mangle.

#### 10.5.1.2. Тема № 2. Маркировка трафика

В рамках темы должна быть изучена маркировка трафика: прямая маркировка пакетов, маркировка пакетов на основе маркировки соединений, а также разница между этими двумя способами.

#### 10.5.1.3. Тема № 3. Выбор цепочки

В рамках темы должны быть изучены правила выбора цепочки для использования Mangle.

#### 10.5.1.4. Тема № 4. Порядок обработки

В рамках темы должны быть изучены принципы, на основе которых выполняется порядок обработки правил в IP Firewall Mangle, в т.ч. должны быть изучены возможности по досрочному прерыванию обработки в цепочке.

#### 10.5.1.5. Тема № 5. Лучшие практики по маркировке трафика

В рамках темы должны быть изучены лучшие практики по маркировке трафика.

#### 10.5.1.6. Тема № 6. Маркировка трафика для IP-телефонии

В рамках темы должны быть изучены принципы маркировки трафика для IP-телефонии.

#### 10.5.1.7. Тема № 7. Маркировка маршрутов

В рамках темы должны быть изучены следующие подтемы:

- маркировка маршрутов для будущего применения в именованных таблицах маршрутизации;
- создание маршрутов непосредственно в таблицах Mangle.

#### 10.5.1.8. Тема № 8. Балансировка нагрузки между двумя интернет-каналами

В рамках темы должны быть изучены правила в таблицах Mangle, которые необходимы для балансировки нагрузки между двумя интернет-каналами.

### 10.5.2. Оценочные материалы

Ниже приведены примеры оценочных материалов, которые используются в модуле № 2.4.

#### 10.5.2.1. Тестирование

Ниже приведены примеры тестовых вопросов, которые используются в модуле:

- Правильно ли выполнена маркировка?
- Правильно ли выполнена маркировка трафика для того, чтобы промаркировать трафик ICMP, проходящий через маршрутизатор?

#### 10.5.2.2. Лабораторные работы

**Лабораторная работа № 2.4.1. Маркировка трафика № 1**

В рамках лабораторной работы должны быть закреплены практические навыки простейшей маркировки трафика.

**Лабораторная работа № 2.4.2. Маркировка трафика № 2**

В рамках лабораторной работы должны быть закреплены практические навыки маркировки трафика.

**Лабораторная работа № 2.4.3. Задача № 1**

В рамках лабораторной работы должно быть закреплено понимание того, что соединение – это двунаправленное явление, и понимание того, в какой момент может быть выполнена перемаркировка трафика.

**Лабораторная работа № 2.4.4. Маркировка трафика № 3**

В рамках лабораторной работы должны быть закреплены практические навыки маркировки трафика.

**Лабораторная работа № 2.4.5. Маркировка трафика № 4**

В рамках лабораторной работы должны быть закреплены практические навыки маркировки трафика.

**Лабораторная работа № 2.4.6. Маркировка маршрута**

В рамках лабораторной работы должны быть закреплены практические навыки создания маршрута в Mangle.

**Лабораторная работа № 2.4.7. Задача № 2**

Лабораторная работа используется для промежуточной аттестации.

В рамках лабораторной работы должны быть закреплены практические навыки изменения правил маркировки трафика для получения заданного результата.

**Лабораторная работа № 2.4.8. Задача № 3**

Лабораторная работа используется для промежуточной аттестации.

В рамках лабораторной работы должны быть закреплены практические навыки изменения правил. А именно должно быть произведено объединение правил для балансировки нагрузки между интернет-каналами и правил маркировки трафика IP-телефонии.

**Лабораторная работа № 2.4.9. Задача № 4**

Лабораторная работа используется для промежуточной аттестации.

В рамках лабораторной работы должны быть закреплены практические навыки диагностики работоспособности правил.

#### 10.5.2.3. Контрольные работы

**Контрольная работа № 2.4.1**

В рамках контрольной работы должны быть проверены навыки поиска ошибок в настройках IP Firewall Mangle.

**Контрольная работа № 2.4.2**

В рамках контрольной работы должны быть проверены навыки поиска ошибок и навыки оптимизации правил в настройках IP Firewall Mangle.

## 10.6. Модуль 3. QoS

### 10.6.1. Содержание модуля

#### 10.6.1.1. Тема № 1. Simple Queue

В рамках темы должны быть изучены параметры Target, Dst. и Max Limit, а также простые очереди (Simple Queue).

#### 10.6.1.2. Тема № 2. Queue Tree

В рамках темы должны быть изучены очереди Queue Tree и Interface Queues.

#### 10.6.1.3. Тема № 3. Режим Burst

В рамках темы должны быть изучены: режим Burst, условия, с помощью которых задаются его настройки: Burst Limit, Brust Threshold и Burst Time, а также принципы вычисления продолжительности работы режима Burst.

#### 10.6.1.4. Тема № 4. Приоритизация трафика

В рамках темы должны быть изучены следующие подтемы:

- принципы манипуляции скоростями;
- параметры Priority и Limit At;
- расчеты в Hierarchical Tocken Bucket;
- практические рекомендации по приоритизации.

#### 10.6.1.5. Тема № 6. Типы очередей

В рамках темы должны быть изучены разновидности очередей, которые могут быть использованы при настройке приоритизации трафика.

#### 10.6.1.6. Тема № 7. Прочее

В рамках темы должны быть изучены вопросы, которые не вошли в другие темы: настройка правил с учетом их влияния на загрузку процессора, распространенные ошибки при проектировании очередей, поле DSCP, принципы выбора интерфейса и др.

### 10.6.2. Оценочные материалы

Ниже приведены примеры оценочных материалов, которые используются в модуле № 3.

#### 10.6.2.1. Тестирование

Ниже приведены примеры тестовых вопросов, которые используются в модуле:

- В какой цепочке находится логический блок QoS?
- Какой тип очереди не обходится с помощью FastTrack?
- Max-limit родительской очереди равен 50 Мбит/с, limit-at трех дочерних очередей равен 15 Мбит/с, 17 Мбит/с и 10 Мбит/с. Какое максимальное значение limit-at можно указать для еще одной, 4-й дочерней очереди?

#### 10.6.2.2. Лабораторные работы

**Лабораторная работа № 3.1. Simple Queue**

В рамках лабораторной работы должны быть закреплены практические навыки настройки простых очередей (Simple Queue).

**Лабораторная работа № 3.2. Queue Tree**

В рамках лабораторной работы должны быть закреплены практические навыки настройки дерева очередей (Queue Tree).

**Лабораторная работа № 3.3. Hierarchical Token Bucket**

В рамках лабораторной работы должны быть закреплены практические навыки настройки дерева очередей (Queue Tree) с учетом различных требований к приоритизации трафика.

**Лабораторная работа № 3.4. Типы очередей**

В рамках лабораторной работы должны быть закреплены практические навыки выбора типов очередей, которые могут быть указаны при настройке деревьев очередей.

**Лабораторная работа № 3.5. Поиск неточностей**

Лабораторная работа используется для промежуточной аттестации.

В рамках лабораторной работы должны быть проверены навыки поиска несогласований в настройках очередей и навыки устранения этих неточностей.

#### 10.6.2.3. Контрольные работы

**Контрольная работа № 6.1. Расчеты в HTB № 1**

В рамках контрольной работы должны быть проверены навыки выполнения расчетов при использовании связки из правил, в которых выполняются различные манипуляции со скоростями.

**Контрольная работа № 6.2. Расчеты в HTB № 2**

В рамках контрольной работы должны быть проверены навыки выполнения расчетов при использовании связки из правил, в которых выполняются различные манипуляции со скоростями.

**Контрольная работа № 6.3. Расчеты в HTB № 3**

В рамках контрольной работы должны быть проверены навыки выполнения расчетов при использовании связки из правил, в которых выполняются различные манипуляции со скоростями.

### 10.7. Итоговая аттестация

Итоговая аттестация проводится в форме лабораторной работы. В рамках итоговой аттестации должны быть проверены навыки настройки:

- основной сети, гостевой сети и демилитаризованной зоны;
- защиты от сканирования портов и DoS-атак;
- доступа к устройству с помощью перебора портов;
- Hairpin NAT;
- маркировки трафика;
- приоритизации трафика с использованием режима Burst и параметров Priority и Limit At.

## 11. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

### 11.1. Учебно-методическое обеспечение

Учебно-методическое обеспечение состоит из видеолекций, тестирования, лабораторных и контрольных работ. Обучение проводится с помощью системы дистанционного обучения Moodle, установленной на сайте http://kursy-po-it.online.

### 11.2. Кадровое обеспечение

**Разработчик программы:** Скоромнов Дмитрий Анатольевич, высшее образование, инженер по специальности «Многоканальные телекоммуникационные системы», сертифицированный тренер MikroTik, обладатель профессиональных сертификатов MikroTik: MTCNA, MTCTCE, MTCRE, MTCSWE, MTCWE, MTCEWE, MTCSE, MTCUME.
**Руководитель программы:** Скоромнов Дмитрий Анатольевич, высшее образование, инженер по специальности «Многоканальные телекоммуникационные системы», сертифицированный тренер MikroTik, обладатель профессиональных сертификатов MikroTik: MTCNA, MTCTCE, MTCRE, MTCSWE, MTCWE, MTCEWE, MTCSE, MTCUME.
**Преподаватель:** Скоромнов Дмитрий Анатольевич, высшее образование, инженер по специальности «Многоканальные телекоммуникационные системы», сертифицированный тренер MikroTik, обладатель профессиональных сертификатов MikroTik: MTCNA, MTCTCE, MTCRE, MTCSWE, MTCWE, MTCEWE, MTCSE, MTCUME.

### 11.3. Самостоятельная работа слушателей

Самостоятельная работа (СР) – обязательный вид познавательной деятельности, в процессе которой происходит формирование оптимального для каждого отдельного слушателя стиля получения, обработки и усвоения учебной информации. Целями самостоятельной работы являются: систематизация, закрепление, углубление и расширение полученных знаний и навыков. Самостоятельная работа должна проводиться слушателем на протяжении всего обучения.

Самостоятельная работа заключается в:

- конспектировании материала;
- повторном изучении пройденного ранее материала;
- повторном прохождении тестирования и повторном выполнении лабораторных работ;
- самостоятельном эмулировании тех или иных ситуаций, которые явным образом не были описаны в лабораторных работах.

### 11.4. Материально-технические условия

#### 11.4.1. Рабочее место слушателя

Для участия в ОП слушатель должен иметь следующее аппаратное и программное обеспечение или его аналоги:

- Персональный компьютер: частота процессора не менее 2 ГГц, 4 Гб ОЗУ, 10 Гб свободного места на ПЗУ, видеоадаптер и выход в сеть Интернет.

- Операционная система: Microsoft Windows или macOS.
- Интернет-браузер: Microsoft Edge, или Google Chrome, или Safari.
- Офисный пакет: Microsoft Office, или Open Office.
- Просмотр pdf-файлов: Adobe Reader
- Архиватор: WinRAR, или 7-zip.
- Система виртуализации: VMware Workstation, Oracle VirtualBox.
- Проигрыватель аудиовидеофайлов: InfoProtector.
- Скорость доступа к сети Интернет: не менее 10 Мбит/с.

### 11.4.2. Оборудование для лабораторных работ

Виртуальные машины MikroTik Cloud Hosted Router.