МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению лабораторных работ
по дисциплине
«ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В методических указаниях содержатся материалы, необходимые для самостоятельной подготовки студентов к выполнению лабораторных работ. В описание работ включены цель работы, порядок ее выполнения, рассмотрены теоретические вопросы, связанные с реализацией поставленных задач, приведена необходимая литература.

Методические указания посвящены курсу «Защита информации в системах беспроводной связи».

Практикум построен на принципе последовательного изучения объекта исследования с развитием и закреплением знаний и навыков работы.

Результаты работы представляются, как правило, в виде файлов, формат и наименование которых определяется требованиями по оформлению.

Каждая работа заканчивается контрольными вопросами, позволяющими провести самоконтроль и укрепить теоретические знания и практические навыки.

Состав и оформление проекта приводится в соответствие с действующими на сегодняшний день нормами и требованиями государственных стандартов РФ.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01.

Задачами освоения дисциплины являются: формирование базовых понятий в области информационной безопасности и защиты информации, осознание места и роли информационной безопасности в системе национальной безопасности РФ и выработка первоначальных практических навыков по защите документов на персональном компьютере.

2. ОБОРУДОВАНИЕ И МАТЕРИАЛЫ

Аппаратные средства: персональный компьютер;

Программные средства Альт Рабочая станция 10, Альт Рабочая станция K, Альт «Сервер», Пакет офисных программ - Р7-Офис.

Учебный класс оснащен IBM-совместимыми компьютерами, объединенными в локальную сеть. Локальная сеть учебного класса имеет постоянный доступ к сети Internet по выделенной линии. Для проведения лабораторных работ необходимо следующее программное обеспечение: операционная система Альт Рабочая станция, пакет офисных программ Р7-Офис.

3. УКАЗАНИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

Перед началом работы следует убедиться в исправности электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, наличии заземления компьютера, его работоспособности.

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать санитарные правила и нормы, гигиенические требования к персональным электронно-вычислительным машинам.

Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается: вешать что-либо на провода, закрашивать и белить шнуры и провода, закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы, выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

Для исключения поражения электрическим током запрещается: часто включать и выключать компьютер без необходимости, прикасаться к экрану и к тыльной стороне блоков компьютера, работать на средствах вычислительной техники и периферийном оборудовании мокрыми руками, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов,

неисправную индикацию включения питания, с признаками электрического напряжения на корпусе, класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.

Во избежание поражения электрическим током, при пользовании электроприборами нельзя касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

После окончания работы необходимо обесточить все средства вычислительной техники и периферийное оборудование. В случае непрерывного учебного процесса необходимо оставить включенными только необходимое оборудование.

4. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1. Проверка на уязвимость OpenSSL сетевых устройств с помощью ScanNow UPn

Цель работы: научиться проверять качество прошивки и адекватность настроек сетевых устройств с помощью ScanNow UPn.

Теоретическая часть

OpenSSL — это криптографический инструментарий, реализующий сетевые протоколы Secure Sockets Layer (SSL v2/v3) и Transport Layer Security (TLS v1) и соответствующие им стандарты криптографии.

Программа **openssl** — это инструмент командной строки для использования различных криптографических функций криптографической библиотеки OpenSSL в консоли. Основны возможности:

- Создание и управление закрытыми ключами, открытыми ключами и параметрами.
- Криптографические операции с открытым ключом
- Создание сертификатов X.509, CSR и CRL
- Расчёт дайджестов сообщений
- Шифрование и дешифрование с помощью шифров
- Клиентские и серверные тесты SSL/TLS
- Обработка подписанной или зашифрованной почты S/MIME
- Запросы отметок времени, генерация и проверка

Как работают SSL сертификаты

Сгенерированные в OpenSSL ключи могут использоваться для шифрования различных данных, но самое популярное использование — шифрование в HTTPS протоколе, где используется ассиметричное шифрование, это означает, что для шифрования используется один ключ, а для расшифровки — второй ключ. Эти ключи называются:

- приватный ключ
- публичный ключ

Как можно понять из названия, публичный ключ не является секретным. Он свободно распространяется и используется для шифрования данных, которые можно расшифровать только приватным ключом.

Публичный и приватный ключ генерируются вмести и криптографически связаны.

Ещё данная пара ключей может использоваться для подписи данных и проверки подписи. Эта подпись подтверждает то, что данные удостоверены владельцем приватного ключа и в последствии эти данные не были изменены. Подписываются данные приватным ключом (которые имеет одно определённое лицо), а проверить подпись можно публичным ключом, который может получить каждый.

Сертификат, по сути, это публичный ключ, а также информация о домене и другая сопутствующая информация, подписанная электронной подписью.

В результате процедура создания сертификата выглядит так:

1. Владельцем сайта генерируется пара приватный и публичный ключ.
2. Публичный ключ вместе с другой информацией для подписи (например, название доменного имени) упаковывается в файл в специальном формате. Он называется — Certificate Signing Request (CSR), то есть «запроса на подпись сертификата».
3. Данный запрос на подпись (CSR) отправляется в Центр Сертификации (CA), который, используя свой приватный корневой ключ, создаёт подпись для этих данных и всё это упаковывается в другой специальный файл, называемый сертификат.

В результате получается сертификат со следующими свойствами:

1. Он может зашифровать данные (в нём есть публичный ключ), которые способен расшифровать только приватный ключ составляющий пару этому сертификату
2. Сертификат может быть проверен на подлинность (у него есть цифровая подпись) с помощью сертификата Центр Сертификации (CA), который его создал

При подключении к сайту пользователи получают свою копию сертификата этого сайта, и браузер автоматически проверяет её по доверенным корневым сертификатам, которые содержаться в операционной системе или хранятся в веб браузере.

После этого браузер шифрует с помощью сертификата сайта данные и отправляет их на сервер, эти данные может расшифровать только владелец приватного ключа, то есть сервер. Таким образом происходит согласование ключа, используемого для последующего шифрования.

Как генерировать сертификаты в OpenSSL

На самом деле, приватный ключ веб-сервера и приватный ключ Центр Сертификации (CA) по своей природе ничем не отличаются — они генерируются одной и той же командой. Но Центр Сертификации (CA) имеет особый статус постольку:

1. Его приватный ключ используется для подписи сертификатов (поэтому он называется корневым, хотя в физическом смысле не отличается от приватного ключа сервера)
2. Его публичный ключ (сертификат) добавлен на компьютеры всех пользователей в качестве доверенного
3. Цифровая подпись в сертификате не предназначена для проверки третьей стороной, поскольку сертификат является самоподписанным. Единственное отличие самоподписанного сертификата из Центр Сертификации (CA) от того, который вы можете сгенерировать сами, в том, что он у вас размещён среди доверенных (в операционной системе или в браузере). Вы можете самостоятельно созданный самоподписанный сертификат разместить среди доверенных, и он будет иметь точно такую же силу как и корневой сертификат из Центр Сертификации (CA)

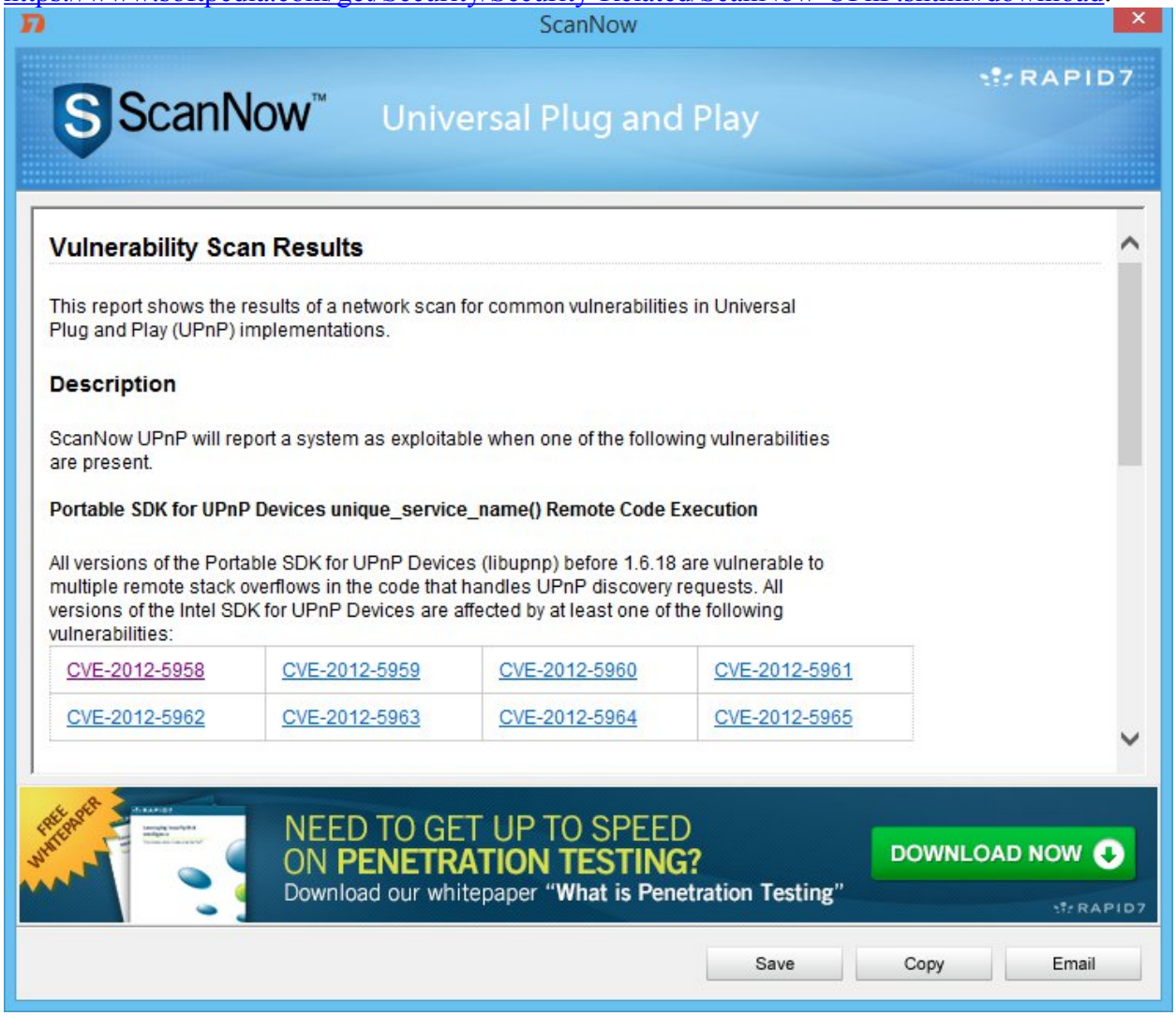
Вернёмся к процедуре подписи, а фактически создания сертификата сервера — создаваемый сертификат должен быть криптографически связан с приватным ключом сервера. Но приватный ключ должен быть известен исключительно его владельцу (серверу). Выходом из данной ситуации является использования уже упомянутого Certificate Signing Request (CSR), то есть «запроса на подпись сертификата». То есть Центру Сертификации передаеъётся публичный ключ и название домена, но приватный ключ остаётся в тайне. Именно в этом смысл существования CSR.

В учебных целях вы можете создать свои корневые ключи и даже свой «Центр Сертификации (CA)». Затем создадим пару приватный и публичный ключ сервера. Используя ключ сервера мы создадим запрос на подпись сертификата (CSR). Приватным ключом CA мы подпишем (создадим) сертификат для сервера.

Также мы научимся добавлять свой корневой сертификат в доверенные, проверять и управлять уже присутствующими доверенными сертификатами.

Сегодня роутеры — приоритетная цель сетевых атак, позволяющая украсть деньги и данные в обход локальных систем защиты. Как самому проверить качество прошивки и адекватность настроек. ScanNow — это бесплатный инструмент, который позволяет вам проверять, можно ли использовать ваши устройства, и помогает снизить риск, связанный с этими уязвимостями.

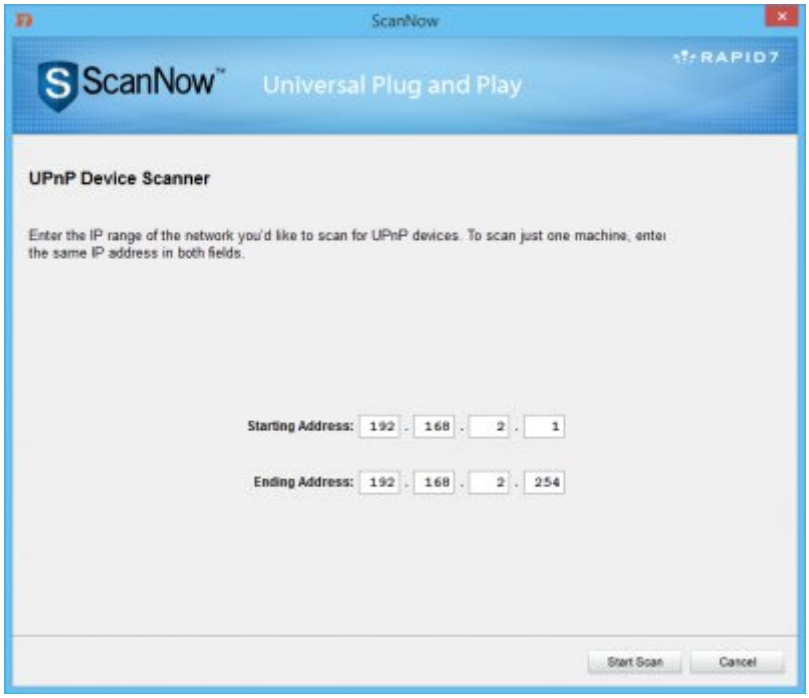
Для проверки наличия уязвимостей в сетях для устройств будет примняться ScanNow — это бесплатный портативный инструмент, который позволяет сканировать протокол Universal Plug and Play (UPnP) и проверять, готовы ли ваши сетевые устройства противостоять уязвимостям или нет. Это очень простой инструмент, но выполняет очень сложную задачу. Утилиту ScanNow фирмы Rapid7 можно скачать по ссылке: https://www.softpedia.com/get/Security/Security-Related/ScanNow-UPnP.shtml#download.



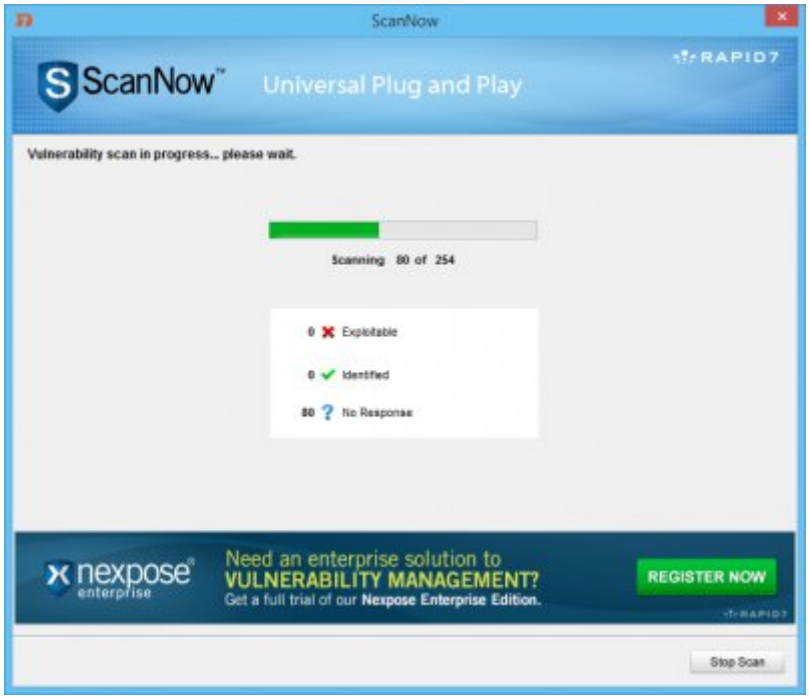
Ход выполнения работы

Перед запуском сканирования вам необходимо зарегистрировать программное обеспечение.

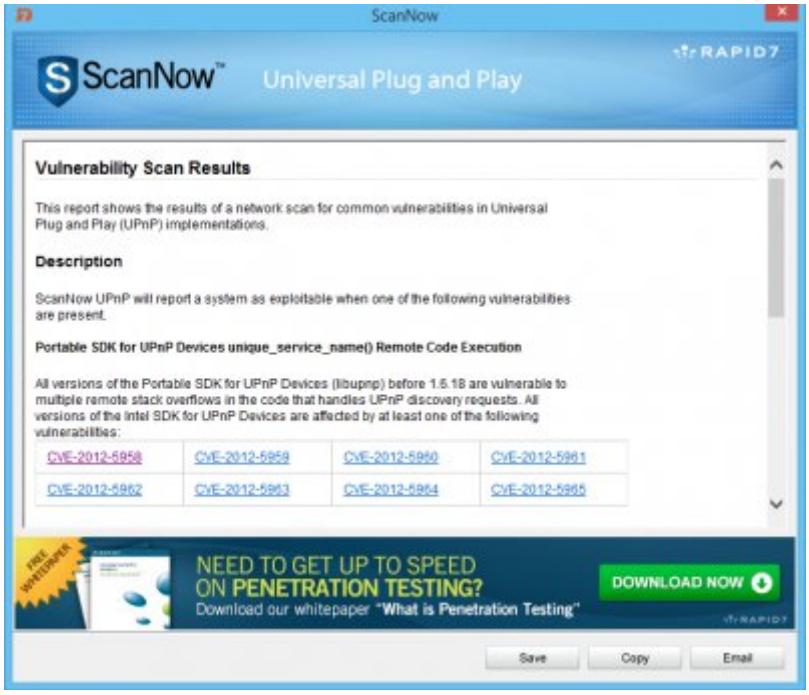
На самом первом экране вам нужно ввести диапазон сетевых IP-адресов, которые вы хотите сканировать на предмет устройств UPnP. Если вы не понимаете шаг, вы можете просто щелкнуть *Начать сканирование,* и он автоматически загрузит диапазон IP на первом шаге.



После того, как сканирование началось, подождите некоторое время, чтобы оно завершилось, оно не займет более 2-3 минут. Если хотите, вы также можете остановить сканирование между ними. После завершения сканирования появится всплывающий отчет с результатами сканирования.



В отчете будут упоминаться уязвимости, и он будет помечен как Exploitable. После упоминания всех возможных уязвимостей отчет подходит к концу, где отображается Обзор результатов, показывающий используемые и идентифицированные устройства в пределах просканированного диапазона IP-адресов.



Сохраните отчет, чтобы использовать предложения для обеспечения безопасности вашего компьютера и защиты от рисков использования. Помните, что инструмент не может исправить проблемы, поскольку они связаны с оборудованием. Он может только предложить профилактические меры, чтобы избежать рисков.

Задание

Для выполнения лабораторной работы необходимо:

1) Провести сканирование.
2) Получить результатами сканирования.
3) Предложить меры защиты.
4) Оформить отчёт.
5) Ответить на контрольные вопросы.
6) Сделать вывод.

Контрольные вопросы:

1. Что такое OpenSSL?
2. Для чего используется OpenSSL?
3. Как работают SSL сертификаты?
4. Как генерировать сертификаты в OpenSSL?

Список литературы

Перечень основной литературы:

1. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. – М: РадиоСофт, 2010, - 255 с., 44 ил.

Перечень дополнительной литературы:

1 Сюваткин В.С. и др. WiMAX – технология беспроводной связи: основы теории , стандарты, применение / Под ред. Крылова В.В. – СПб.: БХВ-Петербург, 2005. – 368с.: ил.

2. Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильям», 2003. – 640 с.

3. Владимиров, А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / Андрей А. Владимиров, Константин В. Гавриленко, Андрей А. Михайловский; пер. с англ. АА. Слинкина. — М.: НТ Пресс, 2005. — 463, [1] с: ил.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.

2. ЭБС «IPRbooks». http://www.iprbookshop.ru.

3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

Практическая работа №2. Контроль доступа по MAC-адресам для беспроводной сети Wi-Fi

Цель работы: научиться настройке контроля доступа по MAC-адресам для беспроводной сети Wi-Fi версии ОС NDMS 2.11 и более ранних.

Теоретическая часть

Что такое функция фильтрации MAC-адресов в маршрутизаторе. Его миссия - ограничить доступ к сети конкретное устройство или группа компьютеров. Например, предположим, что у нас есть компьютер, и мы не хотим, чтобы он подключался к домашней сети. Нам нужно знать его MAC-адрес и создать фильтр на маршрутизаторе.

Имейте в виду, что у нас есть все больше и больше компьютеров подключаются в Интернет. В этом есть свои преимущества, но могут возникнуть и проблемы. В последнем мы можем назвать возможные ошибки из-за слишком большого количества подключенных устройств, а также большего риска для безопасности.

Особенно вам следует подумать о том, что известно как Интернет вещей, которые представляют собой все домашние устройства, которые мы подключили к сети. Мы говорим, например, о телевизорах, роботах-пылесосах, лампочках, видеоплеерах. Все они подключаются по беспроводной сети (или некоторые с помощью кабеля), и мы можем создавать различные фильтры, разрешающие или запрещающие их подключение.

Мы могли бы создать фильтрацию MAC-адресов в маршрутизаторе, чтобы определенные устройства невозможно соединиться, когда мы его активируем. Например, если мы собираемся находиться вдали от дома на долгое время и не хотим, чтобы телевизор или какое-либо устройство подключалось к маршрутизатору, это может создать проблему безопасности в случае появления уязвимости.

Как работает фильтрация MAC-адресов. Современные маршрутизаторы часто включают эту встроенную функцию. Мы сможем создать как белые, так и черные списки в зависимости от того, что мы хотим. В первом случае мы бы добавили устройства в список, и все они без проблем получили бы доступ к сети. Во втором случае все наоборот: мы добавляем устройства, чтобы они не могли подключиться.

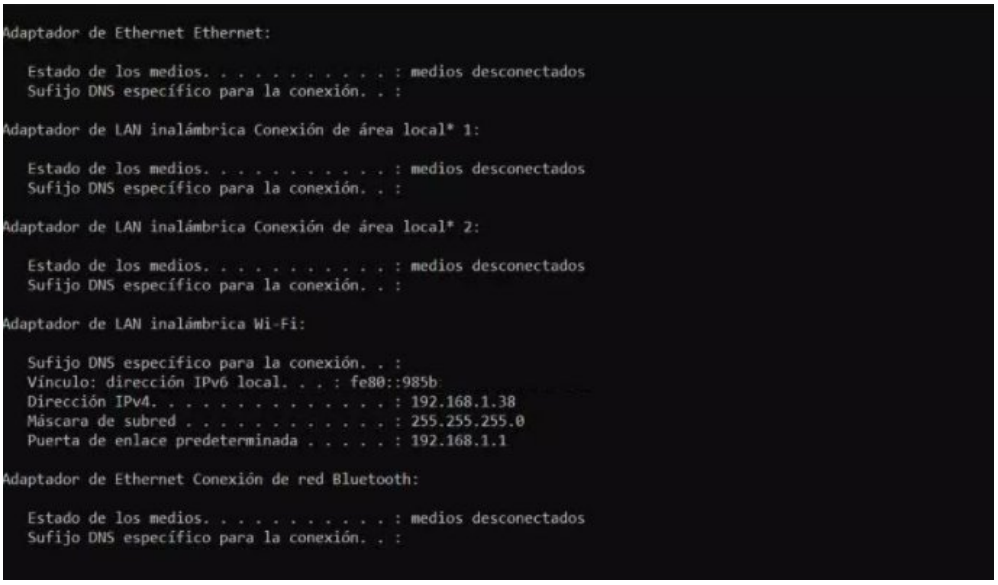
Следовательно, фильтрация MAC-адресов имеет двоякий подход. Если нас интересует только блокировка определенного устройства или нескольких, лучше всего создать черный список и включить их. С другой стороны, если мы хотим заблокировать все подключения и разрешить только компьютеры, которым мы доверяем, нам придется создать белый список и включить их в него.

Маршрутизатор делает идентифицировать каждое устройство в соответствии с его MAC-адресом. Если вы обнаружите, что этот адрес есть в любом списке, который мы создали, тогда вы должны действовать. Этот адрес уникален для каждой сетевой карты устройства. Например, простые умные часы с Wi-Fi будут иметь уникальный MAC.

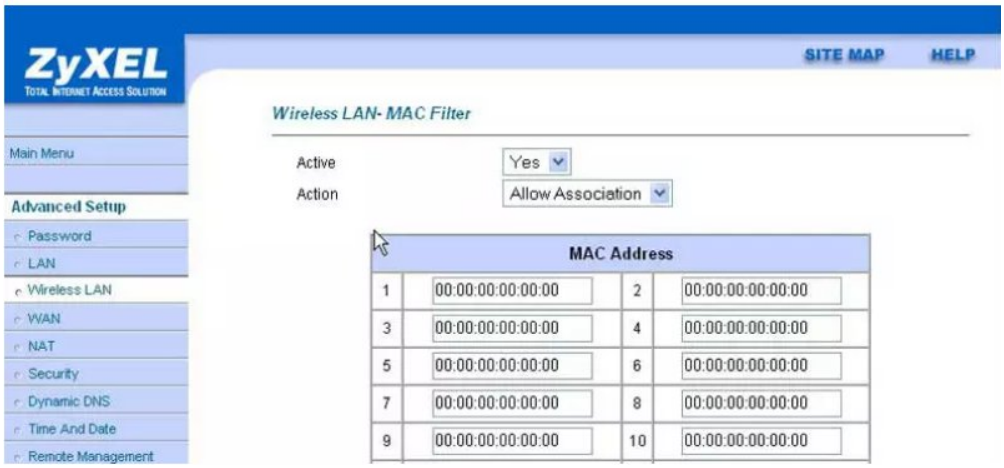
Создать фильтрацию MAC на роутере и запретить подключение определенных устройств очень простой процесс, хотя он может незначительно отличаться в зависимости от типа имеющегося у нас устройства. Мы увидим общие шаги, которые мы должны предпринять для создания списка.

Первое, что нужно сделать, это доступ к роутеру. Мы можем сделать это через шлюз по умолчанию, но также во многих моделях это возможно из вашего собственного приложения. Если мы используем шлюз, мы должны знать, что это такое. Обычно это 192.168.1.1, а затем вводите данные, но они могут быть разными.

Нам нужно перейти в Пуск, войти в командную строку и выполнить IPCONFIG команда. Это покажет нам ряд данных, среди которых есть шлюз по умолчанию. Нам просто нужно поместить его в браузер с соответствующими данными, и мы получаем доступ к устройству.



Оказавшись внутри, это будет зависеть от маршрутизатора. Нормальным является то, что мы должны перейти к Wi-Fi или беспроводной сети и Безопасность. Там появится опция MAC Filtering или MAC Filter. Мы должны активировать его и проверить, хотим ли мы создать список, чтобы заблокировать эти адреса или разрешить их (белый или черный список). Вы должны ввести соответствующие MAC-адреса.



Действительно ли фильтрация MAC защищает нас? Этот момент, несомненно, очень важен и требует подробного разъяснения. Мы можем рассматривать это как дополнительный барьер безопасности для пароля. В каком-то смысле это так, но это не эффективно. Если это неопытный пользователь, который просто знает, какой у нас пароль, из-за какой-то ошибки, например, когда он видел пароль под маршрутизатором, этого может быть достаточно, и он не может войти.

Теперь, если это опытный пользователь, которому удалось взломать наш пароль доступа к Wi-Fi, наличие или отсутствие фильтрации MAC-адресов не принесет злоумышленнику большего, чем потеря нескольких секунд. Это неэффективная мера и не будет проблемой для человека, обладающего соответствующими знаниями.

Это так, потому что можно клонировать MAC-адрес компьютера, который подключен к этой сети Wi-Fi, и, таким образом, иметь возможность подключаться без ограничений. Было бы просто необходимо использовать сетевой сниффер для захвата пакетов и определения местоположения подключенных клиентов для получения MAC.

Следовательно, можно сказать, что Фильтрация MAC- на самом деле нас не защищает. Да, это может быть интересно при определенных обстоятельствах, например, когда одно из наших устройств не подключается к сети или не создает базовый барьер, чтобы кто-то без необходимых знаний не мог подключиться.

Однако фильтрация MAC-адресов - это функция, которую мы встретим в большинстве маршрутизаторов на рынке. Либо через шлюз по умолчанию и доступ из браузера, либо через мобильное приложение, мы сможем легко создать белый или черный список. Конечно, если мы стремимся к максимальной безопасности, мы советуем сосредоточить наши усилия на создании надежного и безопасного ключа Wi-Fi, а также на текущем шифровании.

Ход работы

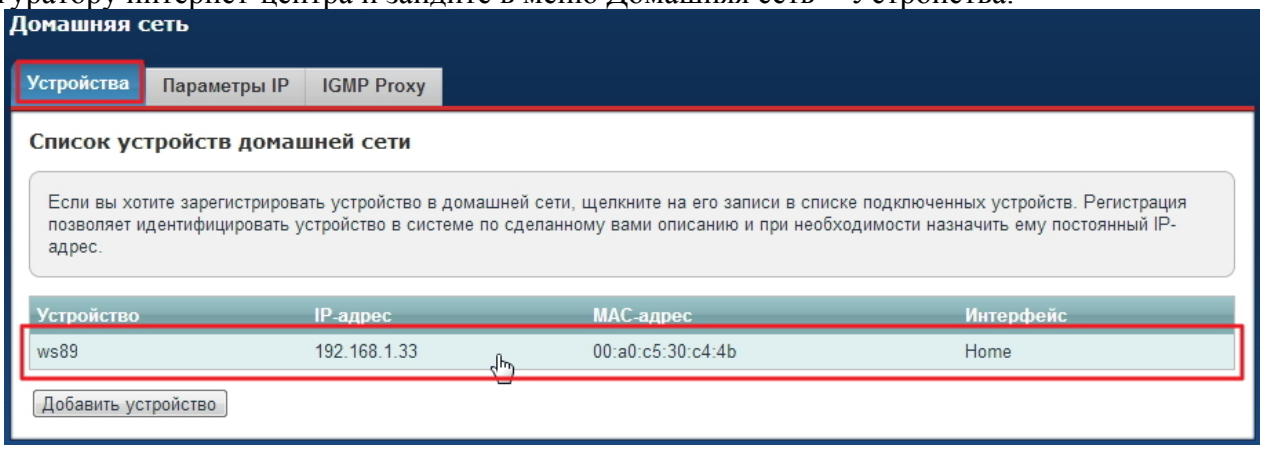
Интернет-центр Keenetic позволяет управлять доступом к беспроводной сети каждого сегмента путем создания списка доступа по MAC-адресам клиентов. Можно создать "Белый" и/или "Черный" список доступа. "Черный список" — блокирует беспроводные клиенты по списку. "Белый список" — блокирует доступ для всех клиентов, не входящих в список.

Списки доступа в сегмент не являются заменой WPA2-аутентификации в беспроводной сети по паролю, рекомендуется использовать их совместно.

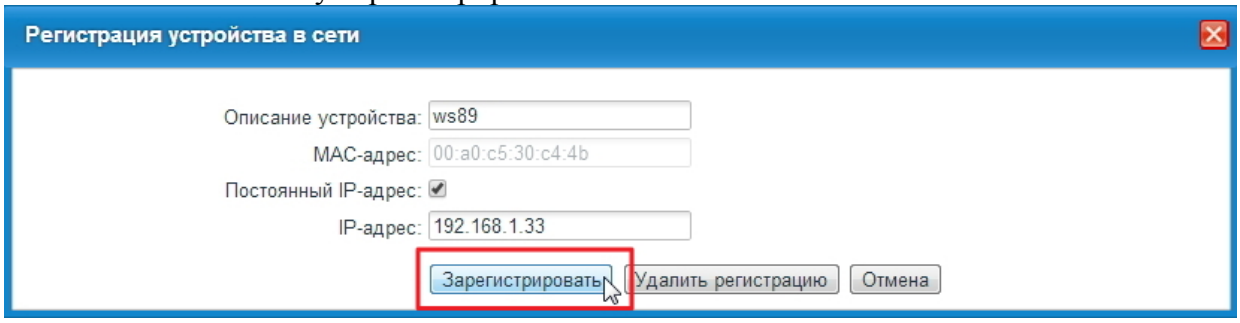
Настроить списки доступа для сетей 2,4 и 5 ГГц можно на странице "Контроль доступа Wi-Fi". Списки доступа по MAC-адресам настраиваются на сегментах и распространяются на интерфейсы точек доступа, включенные в сегмент. Таким образом, вам не нужно будет прописывать новое устройство в двух местах на точках доступа 2,4 и 5 ГГц, а при расширении сети при помощи дополнительных Keenetic в режиме "Точка доступа" или "Усилитель", еще и на этих устройствах. Достаточно будет прописать новое устройство один раз в сегменте "Домашняя сеть".

По умолчанию контроль доступа к сети Wi-Fi по MAC-адресам в интернет-центре не используется.

1. Перед началом настройки списков доступа по MAC-адресам нужно выполнить регистрацию соответствующего устройства в домашней сети. Для этого подключитесь к веб-конфигуратору интернет-центра и зайдите в меню Домашняя сеть > Устройства.



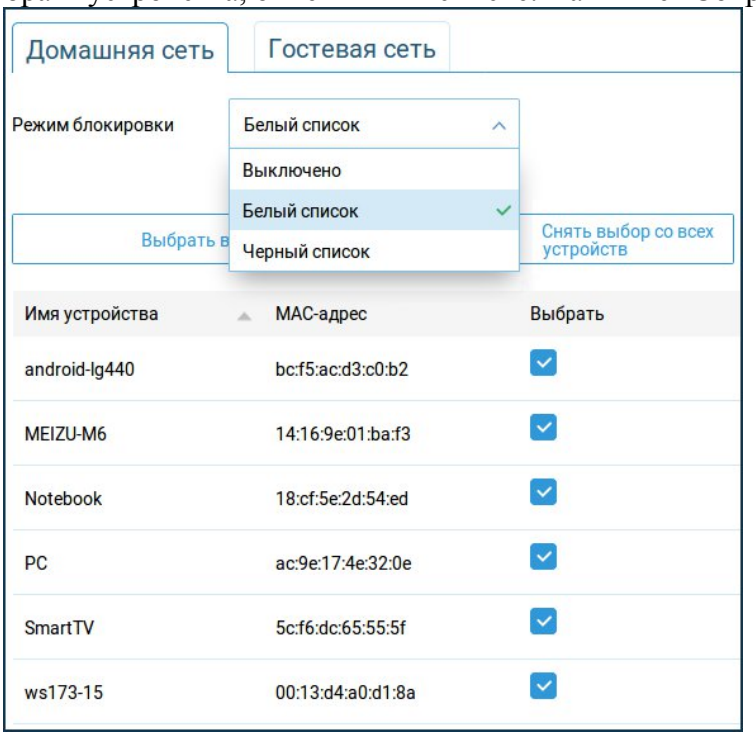
На этом экране вы увидите список подключенных в данный момент сетевых устройств (как по кабелю Ethernet, так и по Wi-Fi). Щелкните мышкой по записи нужного устройства. В появившемся окне Регистрация устройства в сети рекомендуем поставить галочку в поле Постоянный IP-адрес, чтобы данному сетевому устройству назначался постоянный IP-адрес, а затем нажмите кнопку Зарегистрировать.



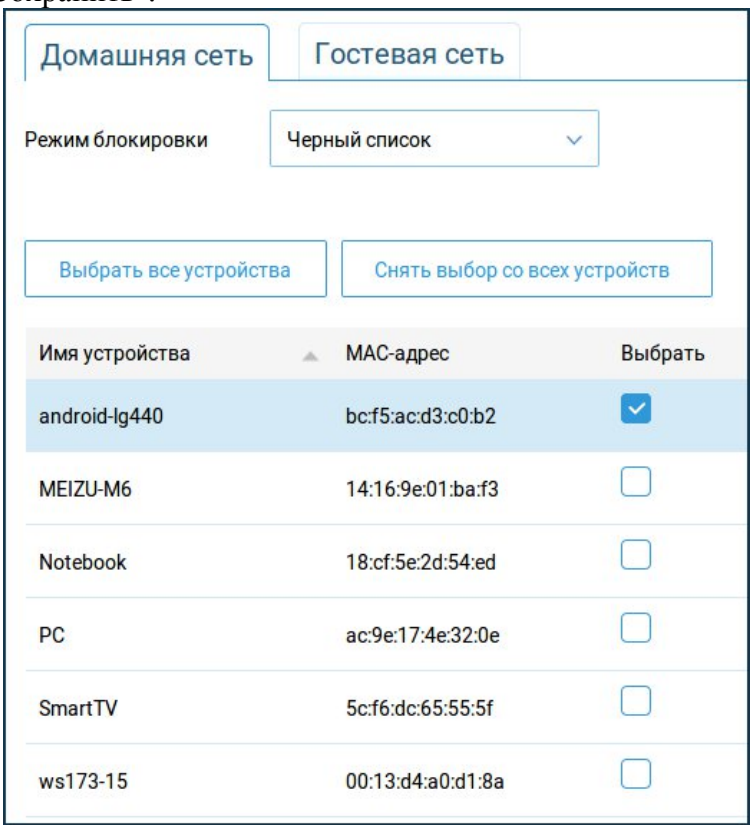
Кроме того, вы можете самостоятельно добавить устройство в список устройств домашней сети, когда оно не подключено к интернет-центру. Для этого нажмите

кнопку Добавить устройство в меню Домашняя сеть > Устройства и самостоятельно заполните поля в окне Регистрация устройства в сети.

2. После регистрации устройства в домашней сети можно перейти к созданию списков доступа. При создании "Белого списка" на вкладке "Домашняя сеть" в поле "Режим блокировки" выберите значение "Белый список". При включении "Белого списка" автоматически выбираются все устройства, зарегистрированные в интернет-центре. Вы можете вручную выбрать устройства, отметив их в списке. Нажмите "Сохранить".



При создании "Черного списка" нужно вручную выбрать устройства, отметив их в списке. Нажмите "Сохранить".



Аналогичным образом настраиваются списки доступа для сегмента "Гостевая сеть" и других созданных сегментов (дополнительных точках доступа) интернет-центра Keenetic.

3. При использовании "Белого списка" и при подключении нового устройства по Wi-Fi временно отключите "Белый список" - в поле "Режим блокировки" установите значение "Выключено". Затем на странице "Список устройств" вы увидите новое незарегистрированное устройство. Зарегистрируйте его и потом вновь включите "Белый список", добавив новое устройство в этот список.

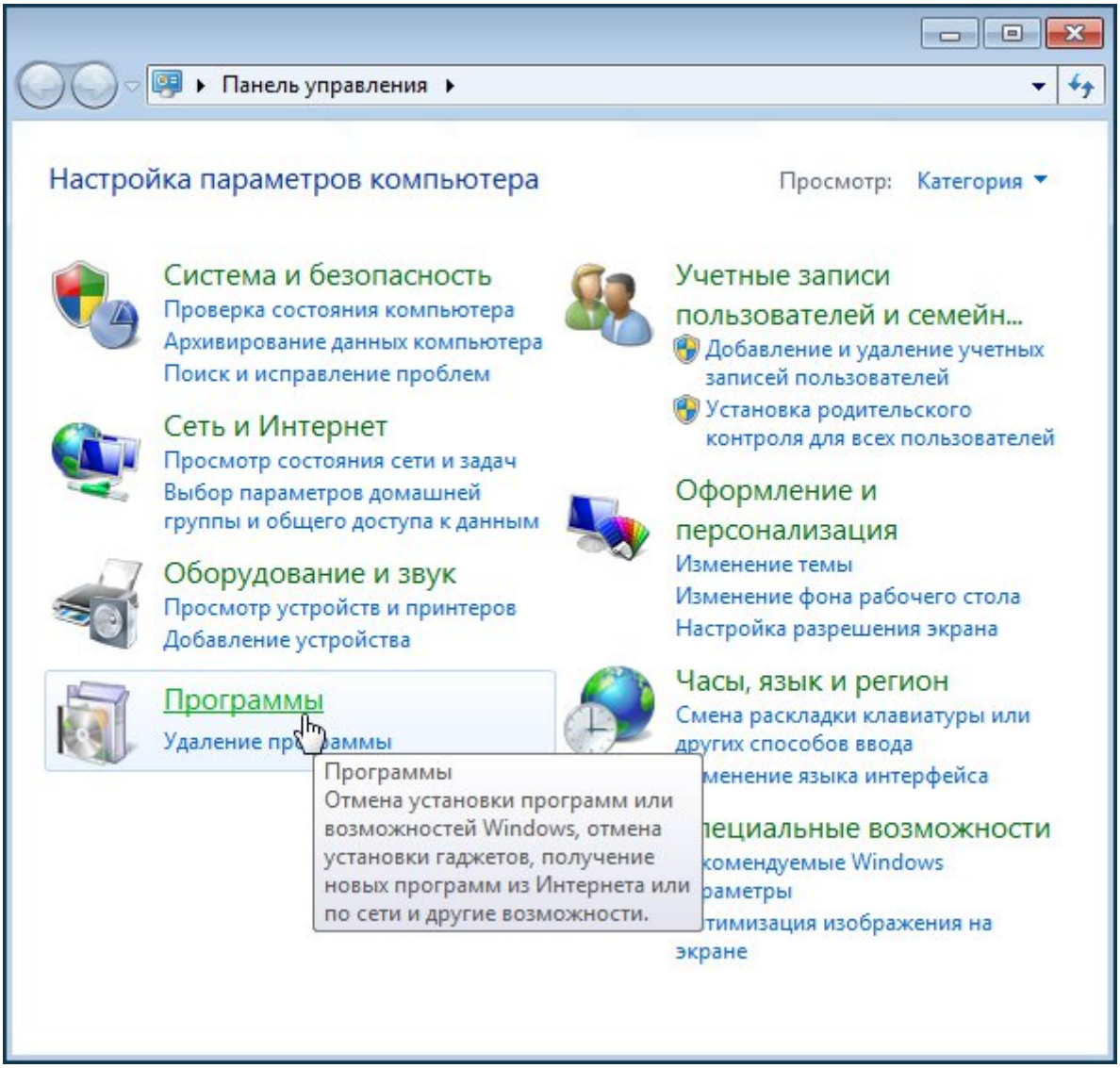
4. Если после включения "Белого списка" перестал подключаться интернет-центр в режиме "Адаптер" или "Усилитель", обратитесь к статье: "Почему дополнительный интернет-центр, работающий в режиме Адаптер/Усилитель не может подключиться к основной точке доступа, после того как он был добавлен в Белый список?"

Начиная с версии KeeneticOS 2.13 изменилась логика создания списков доступа.

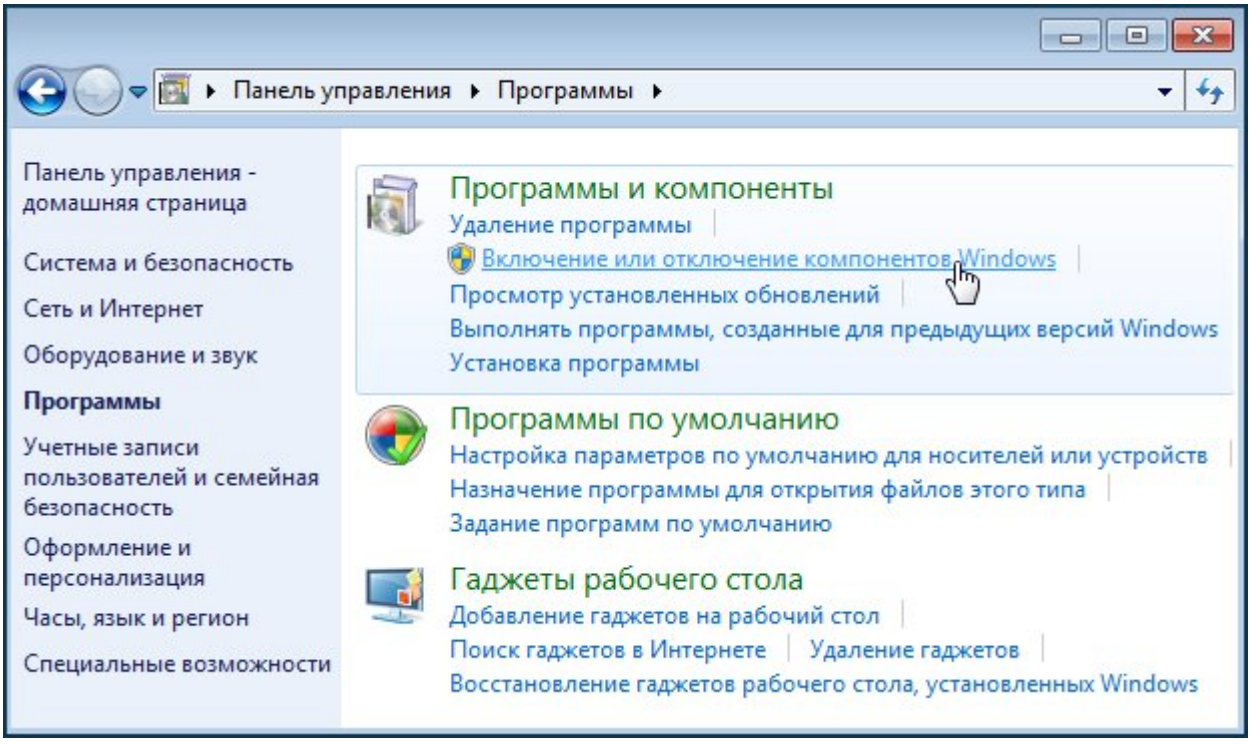
Теперь они создаются на базе уже зарегистрированных устройств и список доступа привязан к сегменту сети, а ранее списки доступа были привязаны к конкретной точке доступа. В версиях 2.13+ настройка индивидуальных списков исчезла из веб-интерфейса, но если они ранее были созданы и включены, то продолжают работать. Списки доступа по MAC-адресам, настроенные на точках доступа в старом веб-интерфейсе, действуют до тех пор, пока не включен список доступа в новом интерфейсе. Чтобы отключить старый список доступа и начать пользоваться новым, достаточно включить список доступа на странице "Контроль доступа Wi-Fi". После этого старые списки будут отключены. Но мы рекомендуем выключить индивидуальный список доступа на точке доступа 2.4 / 5 ГГц. И в дальнейшем пользуйтесь только меню "Контроль доступа Wi-Fi" веб-интерфейса для управлением списками доступа.

5. Интерфейс командной строки (CLI) интернет-центра. Для тонкой настройки интернет-центра предусмотрен профессиональный интерфейс командной строки (CLI — Command Line Interface). Для подключения к интерфейсу командной строки интернет-центра нужно использовать сетевой протокол TELNET/SSH.

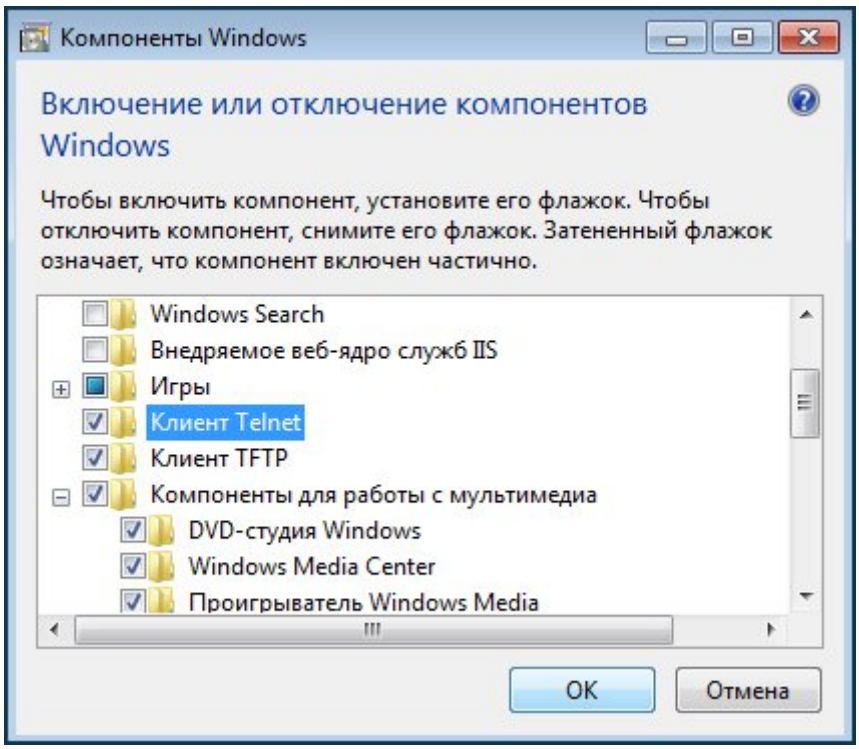
6. Включение служб Telnet и TFTP в Windows. По умолчанию в операционной системе Windows Vista/7/8/10 не установлены компоненты "Клиент Telnet" и "Клиент TFTP". Для установки данных служб зайдите в Панель управления > Программы (Программы и компоненты).



В разделе "Программы и компоненты" нажмите "Включение или отключение компонентов Windows".



В открывшемся окне "Компоненты Windows" отметьте компоненты "Клиент Telnet" и/или "Клиент TFTP".



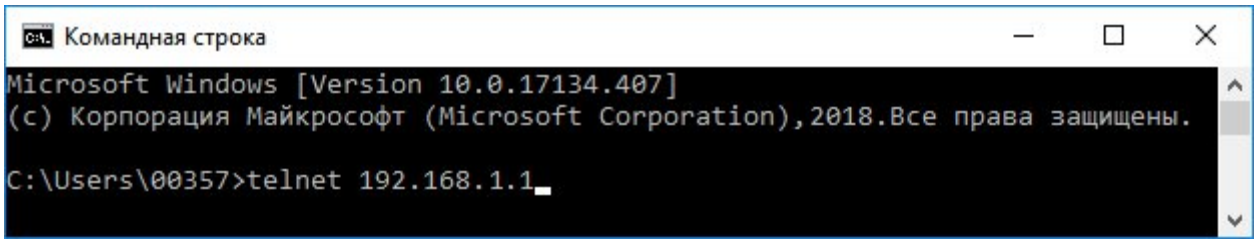
Нажмите кнопку OK и подождите, пока операционная система Windows установит и запустит службу.

Запустите приложение "Командная строка" в операционной системе Windows (в системах Linux/Mac OS запустите "Терминал"). Вы увидите окно командной строки операционной системы компьютера.

По умолчанию в интернет-центре Keenetic предустановлен IP-адрес 192.168.1.1. Для подключения к командной строке интернет-центра введите команду:

telnet 192.168.1.1

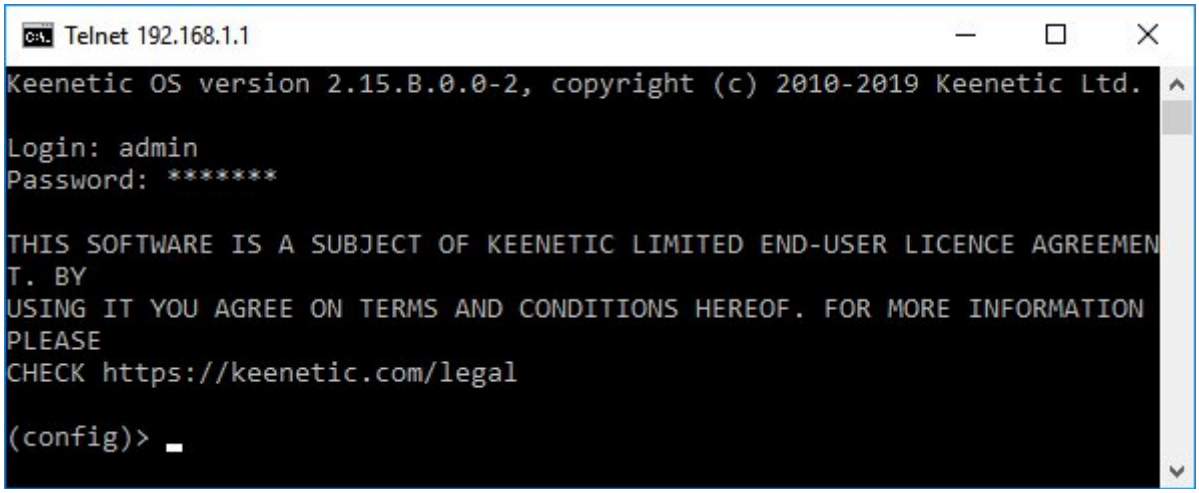
и нажмите Enter.



После этого появится приглашение ввести пароль для входа в настройки интернет-центра.

Чтобы защитить систему от несанкционированного доступа, обязательно установите пароль администратора интернет-центра.

После успешной авторизации, вы увидите интерфейс командной строки (CLI):



Для удобного использования интерфейса командной строки роутера пользуйтесь клавишей Tab. Например, если в приглашении командной строки (config)> нажать клавишу Tab, вы увидите набор доступных команд текущего уровня. Для того чтобы сделать процесс ввода команд максимально удобным, интерфейс командной строки имеет функцию автодополнения команд и параметров, подсказывая пользователю, какие команды доступны на текущем уровне вложенности. Автодополнение работает по клавише [Tab].

(config)> **sys[Tab]**

system - maintenance functions

(config)> system **conf[Tab]**

configuration - manage system configuration

(config)> system configuration **save[Enter]**

Core::ConfigurationSaver: Saving configuration...

Для выхода из интерфейса командной строки (CLI) используйте команду:

(config)> **exit**

В интерфейсе командной строки (CLI) интернет-центра для выключения списка доступа в сети 2.4 ГГц выполните команды:

interface WifiMaster0/AccessPoint0 mac access-list type none
system configuration save

Для выключения списка доступа в сети 5 ГГц:

interface WifiMaster1/AccessPoint0 mac access-list type none
system configuration save

Задание

На лабораторном занятии необходимо:

1) Получить доступ к роутеру.
2) Создать список доступа.
3) Установить компоненты "Клиент Telnet" и "Клиент TFTP".
4) Выключить список доступа в сети 2.4 ГГц и сети 5 ГГц.
5) Оформить отчёт.

6) Ответить на контрольные вопросы.
7) Сделать вывод.

Контрольные вопросы:

1. Что такое MAC-фильтрация маршрутизатора?
2. Как работает фильтрация MAC-адресов?
3. Перечислите шаги по созданию MAC-фильтра.
4. На сколько эффективна фильтрация MAC?

Список литературы

Перечень основной литературы:

1. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. – М: РадиоСофт, 2010, - 255 с., 44 ил.

Перечень дополнительной литературы:

1 Сюваткин В.С. и др. WiMAX – технология беспроводной связи: основы теории , стандарты, применение / Под ред. Крылова В.В. – СПб.: БХВ-Петербург, 2005. – 368с.: ил.
2. Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильям», 2003. – 640 с.
3. Владимиров, А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / Андрей А. Владимиров, Константин В. Гавриленко, Андрей А. Михайловский; пер. с англ. АА. Слинкина. — М.: НТ Пресс, 2005. — 463, [1] с: ил.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

Практическая работа №3. Создание VPN-подключения в ОС Windows 10

.

Цель работы: научиться настраивать роутер Keenetic в качестве VPN-сервера.

Теоретическая часть

Все IP-адреса протокола IPv4 делятся на публичные/глобальные/внешние (их называют "белые") — они используются в сети Интернет, и частные/локальные/внутренние (их называют "серые") — используются в локальной сети.

В сети Интернет используются именно публичные глобальные адреса. Публичным IP-адресом называется IP-адрес, который используется для выхода в Интернет. Публичные (глобальные) IP-адреса маршрутизируются в Интернете, в отличие от частных адресов. Наличие публичного IP-адреса на вашем роутере или компьютере позволит организовать собственный сервер (VPN, FTP, WEB и др.), удаленный доступ к компьютеру, камерам видеонаблюдения, и получить к ним доступ из любой точки глобальной сети. С "белым" IP-адресом можно организовать любой собственный домашний сервер для публикации его в сети Интернет: веб (HTTP), VPN (L2TP/IPSec, PPTP, IPSec, OpenVPN, WireGuard), медиа (аудио/видео), FTP, сетевой накопитель NAS, игровой сервер и т.д.

Примечание: Все публичные серверы и сайты в сети Интернет используют "белые" IP-адреса (например, сайт google.com — 172.217.22.14, DNS-сервер Google — 8.8.8.8, сайт yandex.ru — 213.180.204.11, DNS-сервер Яндекс.DNS — 77.88.8.8). Все публичные IP-адреса в сети Интернет уникальны и не могут повторяться.

Для домашних пользователей провайдер может предоставлять всего один или несколько публичных IP-адресов (как правило, это платная услуга).

Маршрутизатор (роутер, интернет-центр) позволяет устройствам домашней сети использовать для выхода в Интернет один публичный IP-адрес, установленный на WAN-интерфейсе устройства, через который осуществляется подключение к Интернету. Именно этот внешний публичный IP-адрес может быть использован для доступа из Интернета к компьютеру домашней сети, но для этого необходимо использовать проброс портов на роутере.

В связи с тем, что "белых" IP-адресов существует ограниченное количество, а рост числа пользователей Интернета увеличивается, интернет-провайдеры всё чаще используют частные ("серые") IP-адреса, назначаемые абонентам.

Частные внутренние адреса не маршрутизируются в Интернете и на них нельзя отправить трафик из Интернета, они работают только в пределах локальной сети. К частным "серым" адресам относятся IP-адреса из следующих подсетей:

- От 10.0.0.0 до 10.255.255.255 с маской 255.0.0.0 или /8
- От 172.16.0.0 до 172.31.255.255 с маской 255.240.0.0 или /12
- От 192.168.0.0 до 192.168.255.255 с маской 255.255.0.0 или /16
- От 100.64.0.0 до 100.127.255.255 с маской подсети 255.192.0.0 или /10; данная подсеть рекомендована согласно rfc6598 для использования в качестве адресов для CGN (Carrier-Grade NAT)

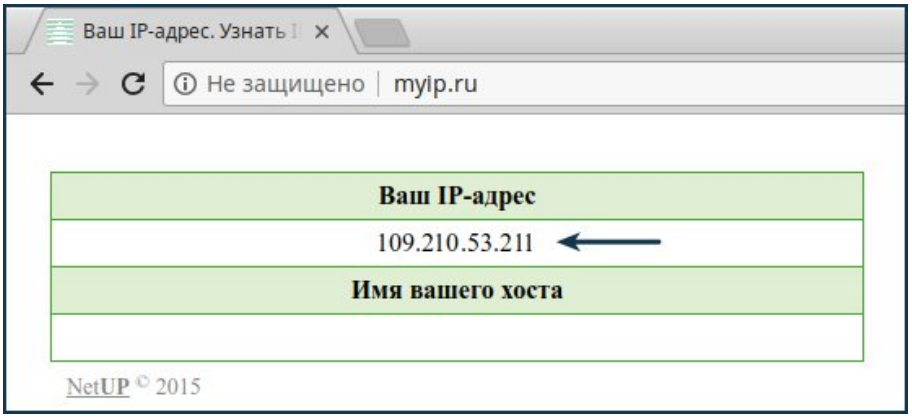
Это зарезервированные IP-адреса. Такие адреса предназначены для применения в закрытых локальных сетях, распределение таких адресов никем не контролируется. Напрямую доступ к сети Интернет, используя частный IP-адрес, невозможен. В этом случае связь с Интернетом осуществляется через NAT (трансляция сетевых адресов заменяет частный IP-адрес на публичный). Частные IP-адреса в пределах одной локальной сети должны быть уникальны и не могут повторяться.

Важно! Если ваш интернет-провайдер предоставляет вам IP-адрес из вышеприведенного списка, то вы не сможете настроить подключение из Интернета к компьютерам и серверам вашей домашней сети (кроме VPN-сервера SSTP и файлового облачного сервера WebDAV), т.к. частные IP-адреса не маршрутизируются (не видны) в сети Интернет. При необходимости доступа к компьютерам вашей домашней сети из Интернета нужно обратиться к интернет-провайдеру для получения публичного "белого" IP-адреса. Но тем не менее, с "серым" IP-адресом вы можете настроить удаленный доступ к веб-конфигуратору интернет-центра и ресурсам (сервисам) домашней сети или интернет-центра через наш сервис доменных имен KeenDNS. Например, доступ к устройству с веб-интерфейсом — сетевому накопителю, веб-камере, серверу, или к интерфейсу торрент-клиента Transmission, работающего в интернет-центре.

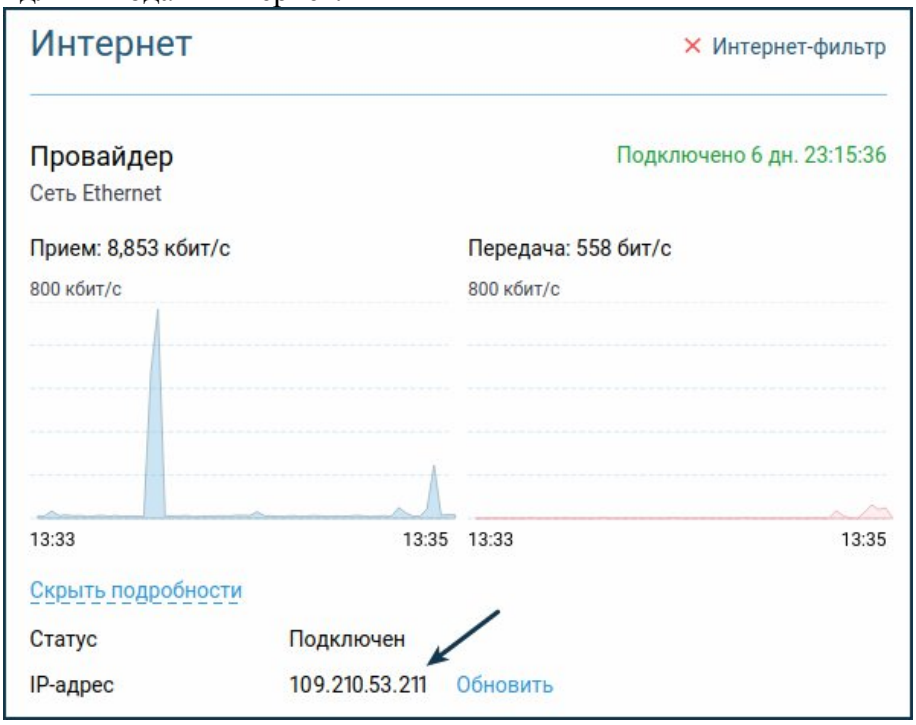
Что касается безопасности в Интернете, то использование "серого" IP-адреса более безопасно, чем использование "белого" IP-адреса, т.к. "серые" IP-адреса не видны напрямую в Интернете и находятся за NAT, который также обеспечивает безопасность домашней сети. При использовании "белого" IP-адреса необходимы меры для обеспечения дополнительной безопасности компьютера или сервера (например, использование межсетевого экрана для блокирования портов и протоколов, которые не используются сервером; применение сегмента сети DMZ для отделения общедоступных сервисов от локальной сети и т.п.).

Полный список описания сетей для протокола IPv4 представлен в документе RFC6890.

Чтобы самостоятельно проверить, является ли ваш IP-адрес публичным "белым", можно воспользоваться сервисом myip.ru, myip.com (или любым подобным). Вам будет показан IP-адрес, под которым был произведен запрос на сайт; если он совпадает с IP-адресом, выданным интернет-провайдером на WAN-интерфейсе интернет-центра, значит, вам выдан публичный "белый" IP-адрес. Например:



IP-адрес на WAN-интерфейсе интернет-центра можно посмотреть в его веб-конфигураторе. На стартовой странице "Системный монитор" в разделе "Интернет" нажмите "Подробнее о соединении". В поле "IP-адрес" вы увидите адрес интернет-центра, используемый для выхода в Интернет.



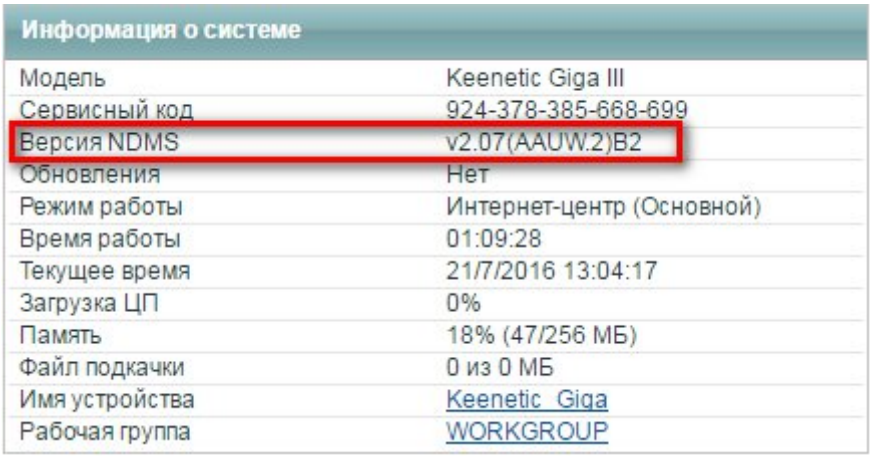
В нашем примере IP-адреса совпадают и этот адрес не входит в диапазон частных подсетей, значит внешний WAN IP-адрес интернет-центра является публичным "белым".

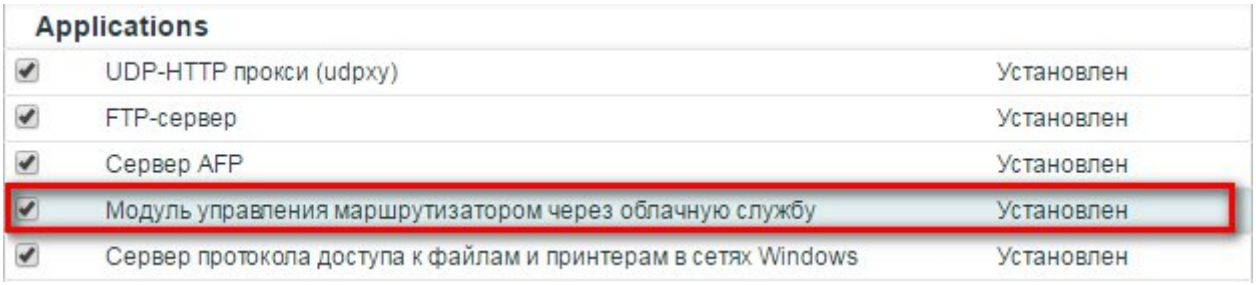
Если вы увидите, что IP-адреса не совпадают, и внешний WAN IP-адрес Keenetic в веб-конфигураторе принадлежит к одному из диапазонов частной сети, значит роутер имеет "серый" IP-адрес.

Ход работы

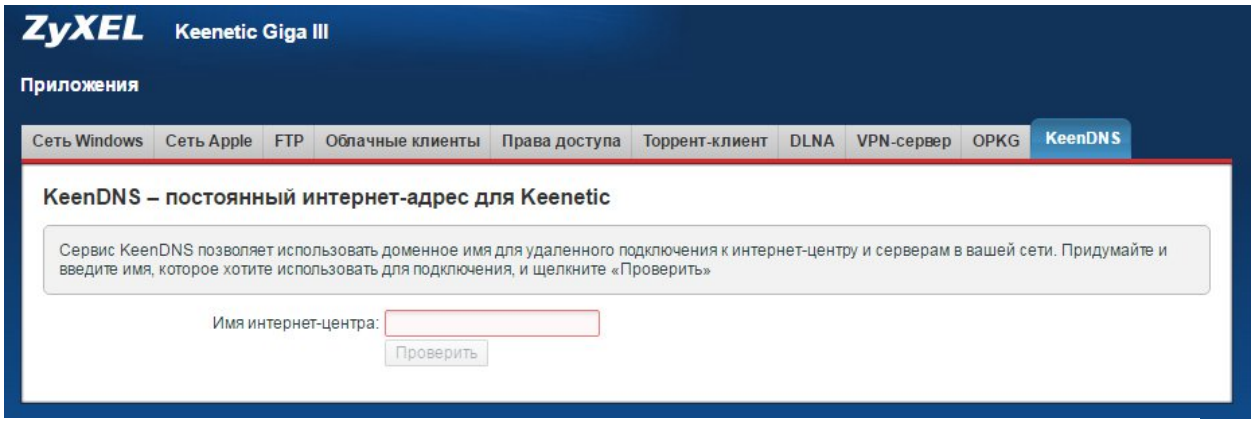
Настройка удаленного доступа к веб-интерфейсу интернет-центра

1. Проверьте, что установлена версия NDMS 2.07.B2 или выше и компонент Модуль управления маршрутизатором через облачную службу.

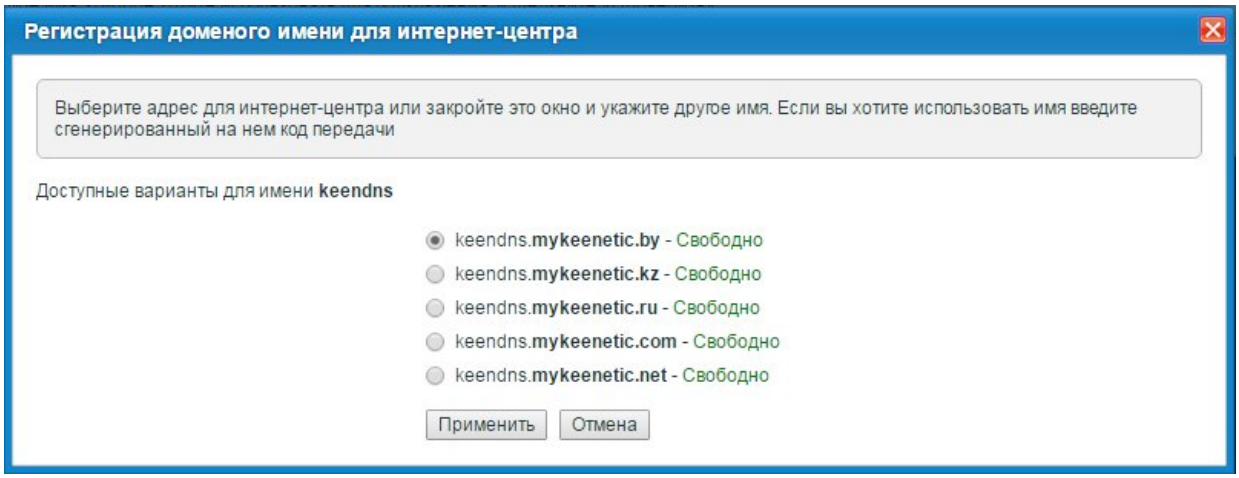




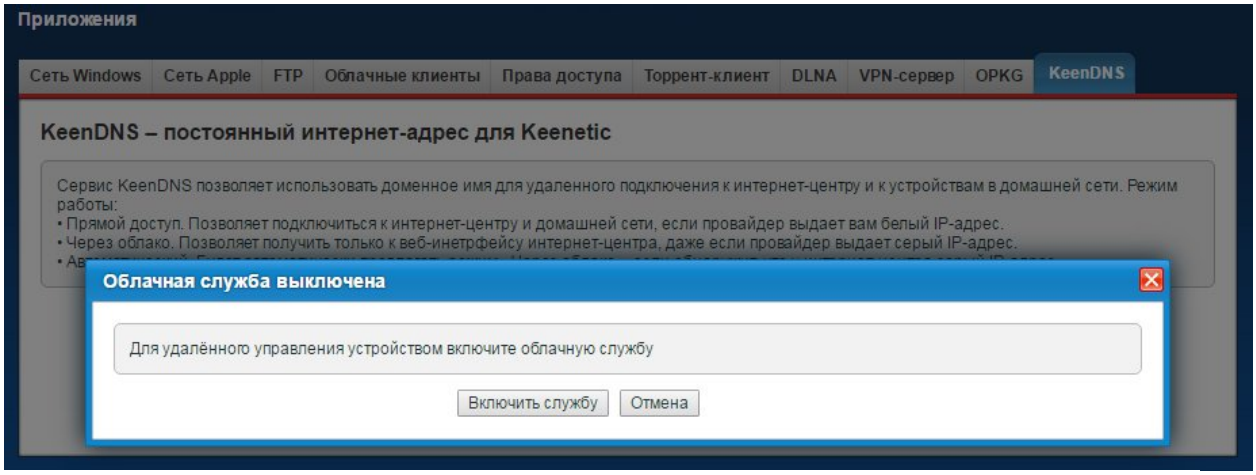
2. Перейдите в меню Приложения > KeenDNS.



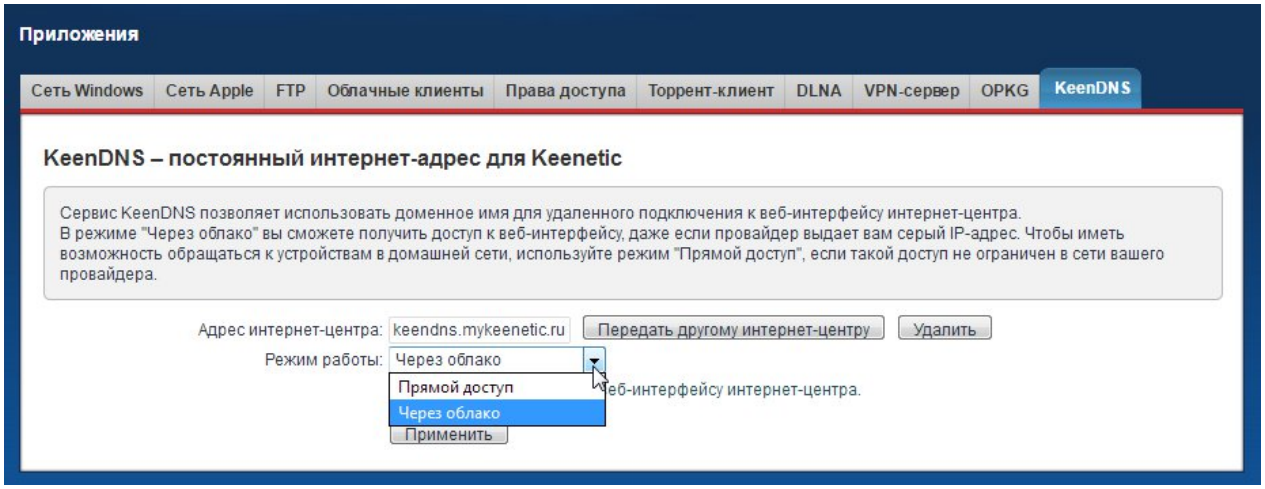
3. Придумайте уникальное имя (постоянный интернет-адрес) для Keenetic, которое будет использоваться для подключения, и впишите его в поле Имя интернет-центра. Затем нажмите кнопку Проверить. Интернет-центр выдаст информацию о доступных и занятых доменах.



4. Выберите один из свободных вариантов и нажмите Применить. Если не включена служба Облачные клиенты, интернет-центр предложит ее включить.



5. После включения облачной службы интернет-центр зарегистрируется на сервере под указанным доменным именем.



Сервис KeenDNS позволяет использовать 2 режима работы:

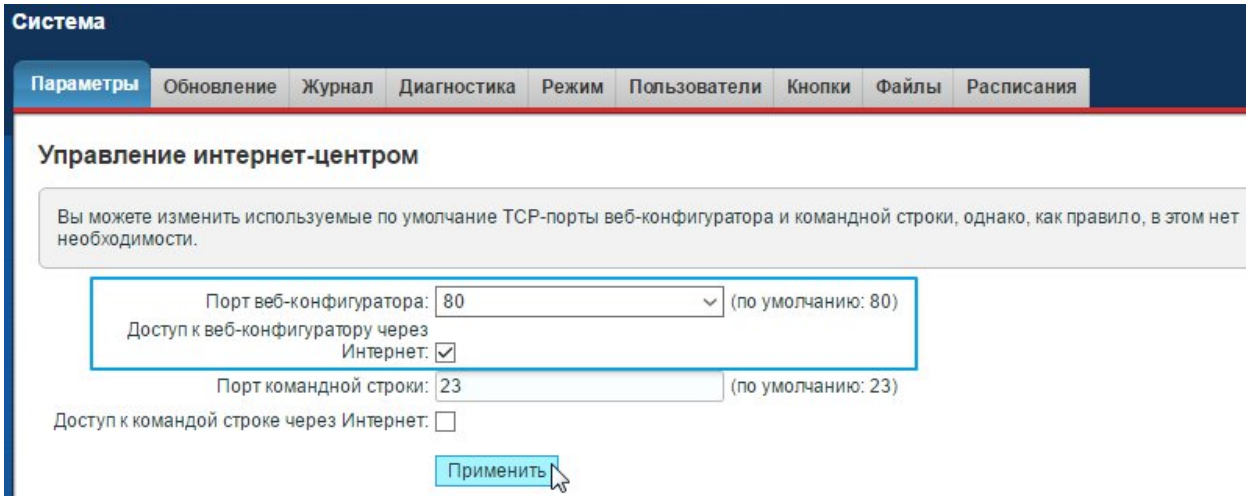
— Прямой доступ (для "белых" публичных IP-адресов);

— Через облако (для "серых" IP-адресов).

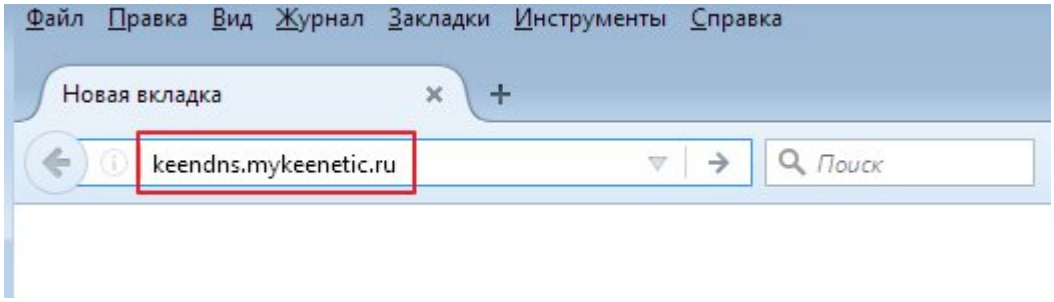
В режиме "Через облако" вы сможете получить доступ только по протоколу HTTP, даже если провайдер выдает вам серый IP-адрес. Чтобы иметь возможность обращаться к устройствам в домашней сети по любому протоколу, используйте режим «Прямой доступ», если такой доступ не ограничен в сети вашего провайдера.

При использовании режима "Через облако" в целях безопасности обязательно установите пароль администратора.

6. Теперь нужно разрешить доступ к интернет-центру из Интернета (по умолчанию он закрыт). Перейдите в меню Система на вкладку Параметры, включите опцию Доступ к веб-конфигуратору через Интернет и нажмите Применить.



7. После произведенных настроек вы сможете обратиться по зарегистрированному доменному имени к веб-интерфейсу интернет-центра из любой точки Интернета.



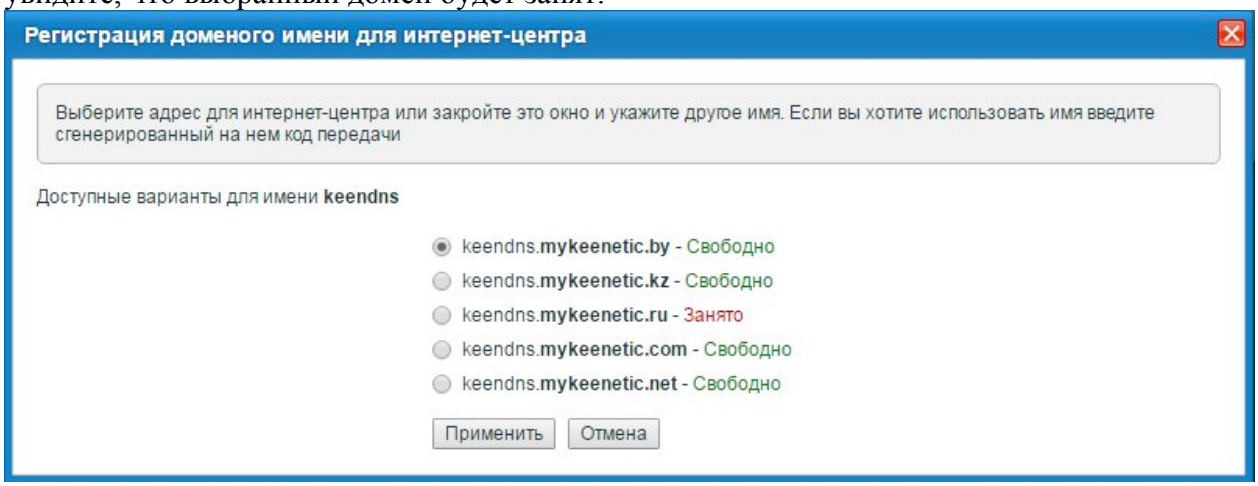
Если на внешнем интерфейсе роутера используется "белый" IP-адрес, для удаленного доступа к веб-интерфейсу интернет-центра дополнительно необходимо разрешить доступ в настройках Межсетевого экрана (для доступа к веб-интерфейсу откройте порт TCP/80 в правилах межсетевого экрана).

При наличии "белого" IP-адреса, помимо режима Прямой доступ, можно использовать режим Через облако.

При наличии "серого" IP-адреса можно использовать только режим **Через облако** и доступ при этом будет возможен только по протоколу **http** на веб-интерфейс интернет-центра (дополнительных правил и разрешений настраивать не нужно).

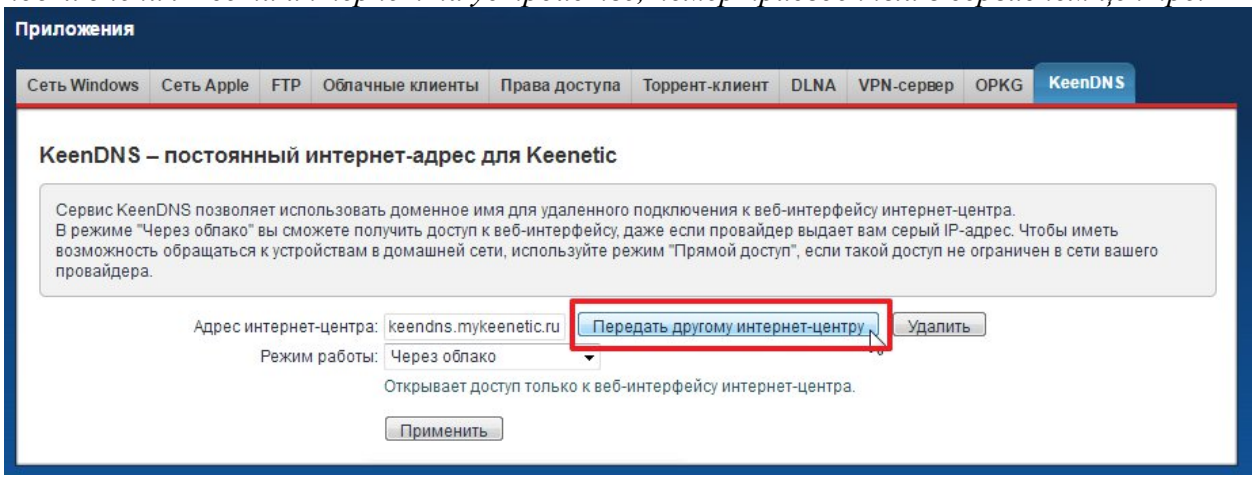
Чтобы перенести зарегистрированное доменное имя с одного интернет-центра на другой, выполните следующие действия:

8. При попытке указать на другом интернет-центре зарегистрированное имя вы увидите, что выбранный домен будет занят.

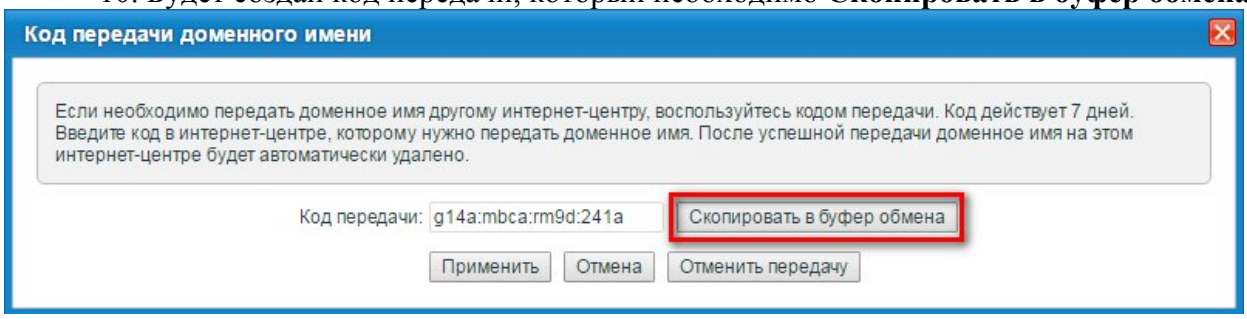


9. Для переноса доменного имени нужно на первом интернет-центре скопировать код передачи, нажав на кнопку Передать другому интернет-центру.

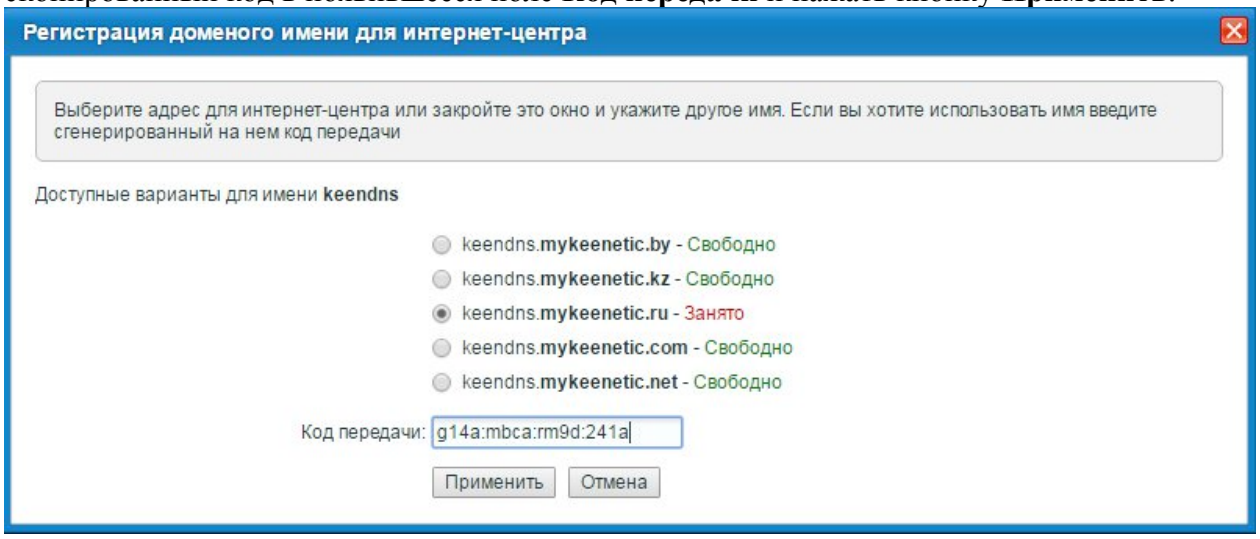
В случае если устройство, например, вышло из строя. то следует подготовить информацию, которая поможет идентифицировать вас как владельца, и обратиться в Техническую поддержку с указанием причины по которой требуется удалить зарегистрированное доменное имя. Пример информации - сервисный код и время последнего подключения к сети интернет на устройстве, номер присвоенный в сервисном центре.



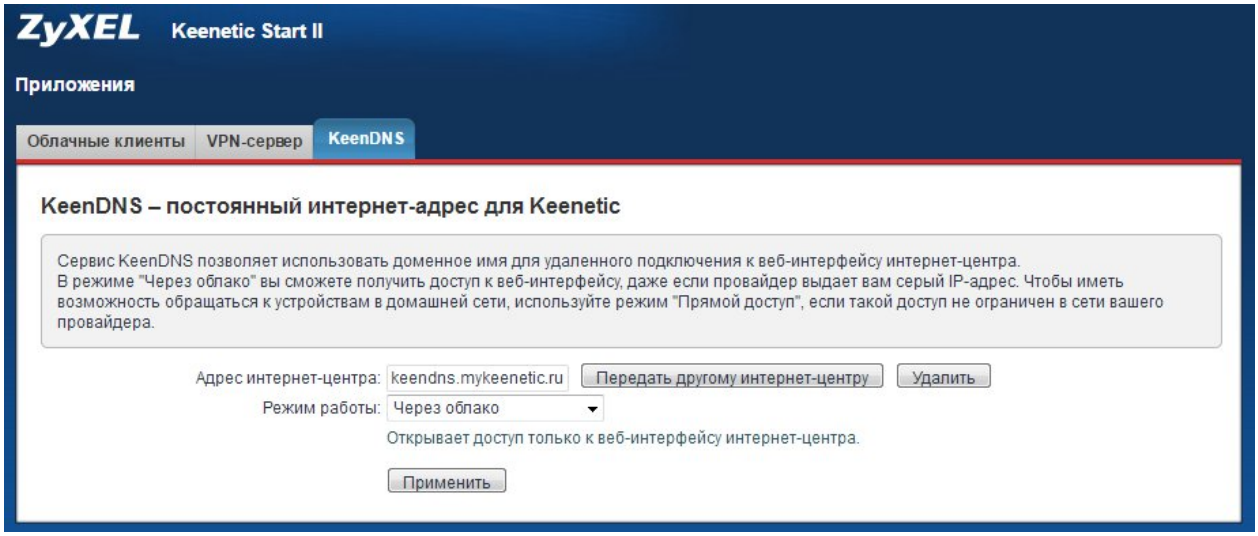
10. Будет создан код передачи, который необходимо **Скопировать в буфер обмена**.



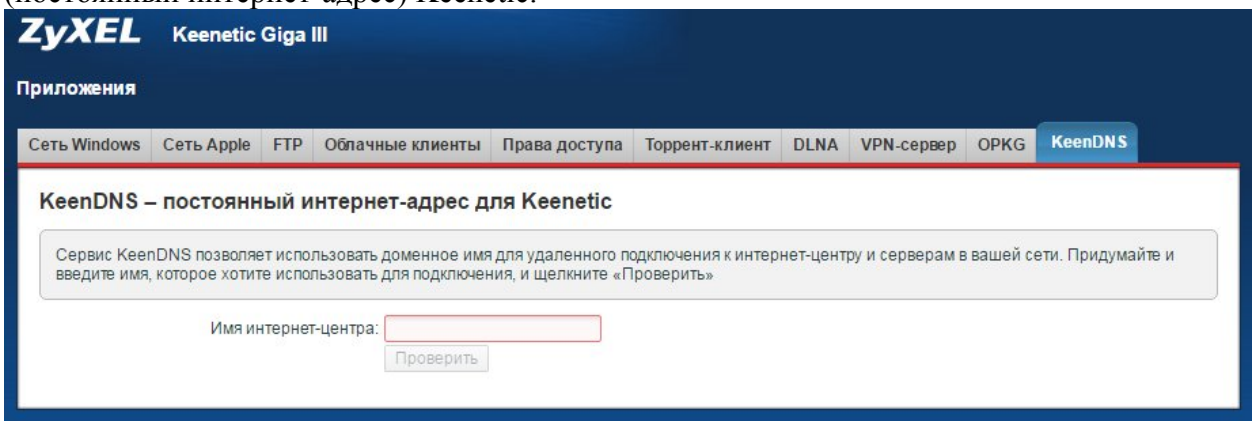
11. На втором интернет-центре необходимо выбрать занятое доменное имя, вставить скопированный код в появившееся поле **Код передачи** и нажать кнопку **Применить**.



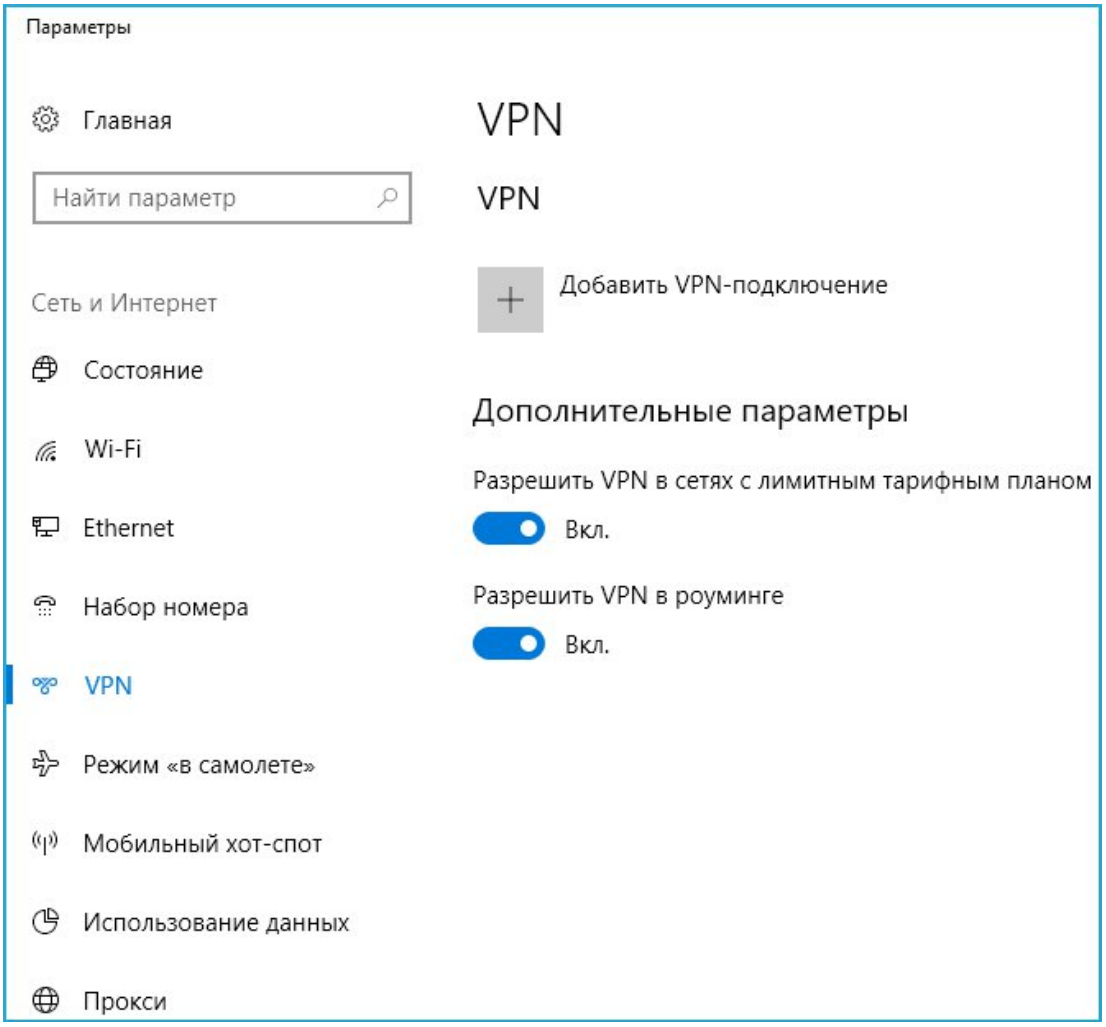
12. После этого доменное имя будет перенесено на второй интернет-центр.



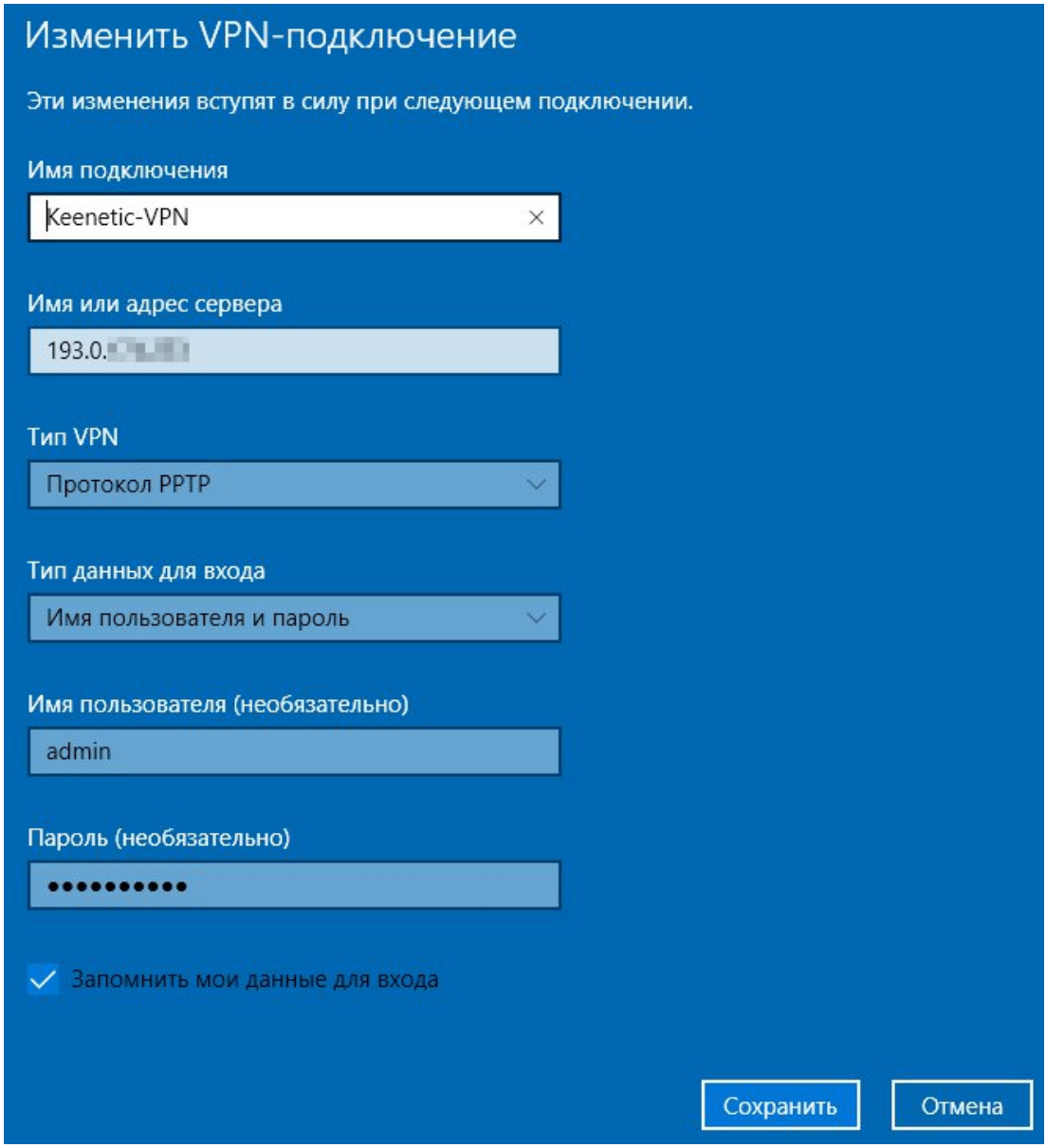
13. Теперь на первом интернет-центре доменное имя указано не будет, т.к. оно было перенесено на второй роутер. При необходимости, вы можете создать новое доменное имя (постоянный интернет-адрес) Keenetic.



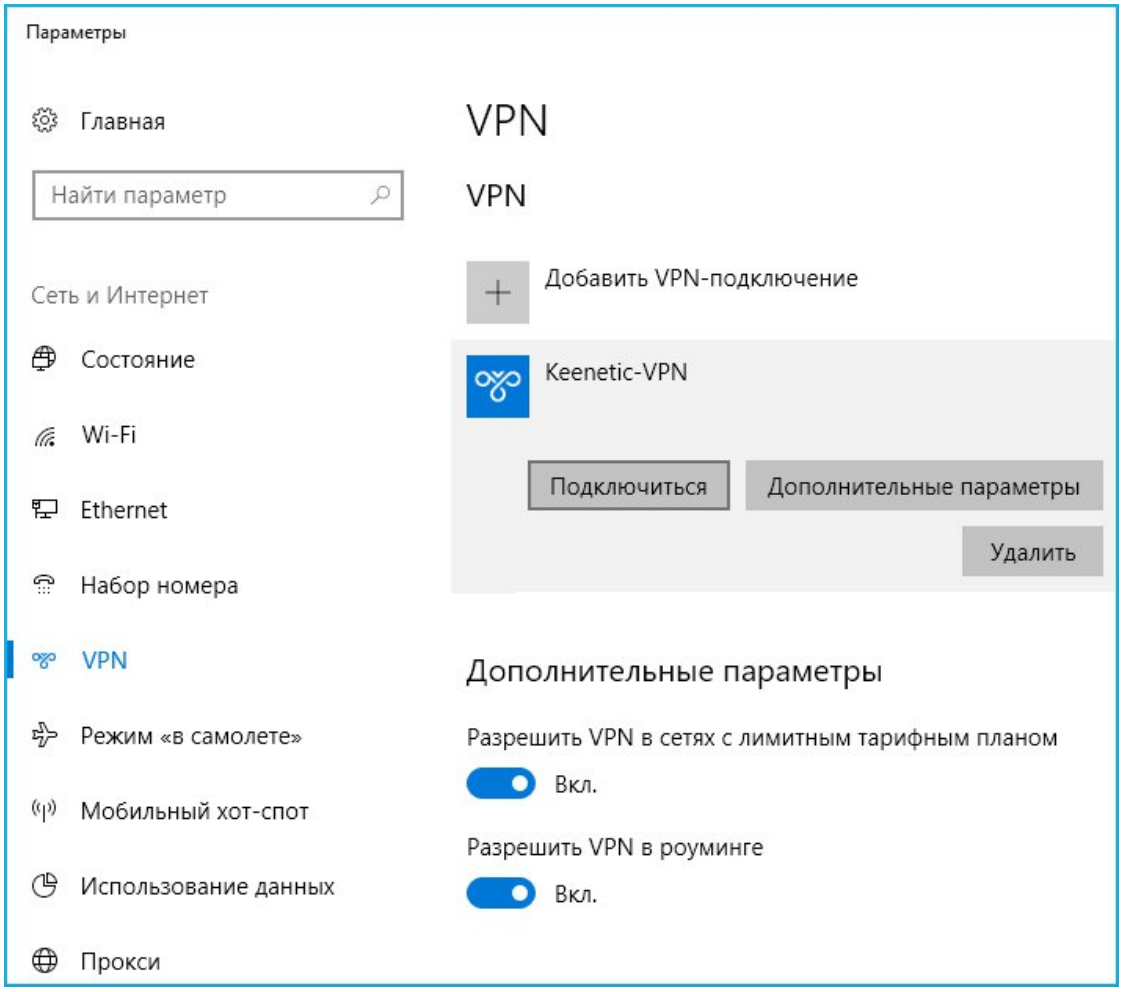
14. Нажмите Пуск > Параметры, перейдите в меню Сеть и Интернет, а затем в раздел VPN. Нажмите кнопку Добавить VPN-подключение.



Создайте VPN-подключение, указав нужные параметры. В поле Имя или адрес сервера укажите публичный "белый" IP-адрес интернет-центра, через который осуществляется подключение к Интернету. В поле Тип VPN укажите значение Протокол PPTP; в поле Тип данных для входа установите Имя пользователя и пароль; в полях Имя пользователя и Пароль соответственно впишите логин и пароль ранее созданной учетной записи интернет-центра, обладающая правами для подключения к VPN-серверу. Установите галочку Запомнить мои данные для входа, чтобы каждый раз при подключении не вводить имя пользователя и пароль. Нажмите кнопку Сохранить.



В разделе VPN появится запись созданного подключения. Для запуска VPN-подключения нажмите на нужную запись и затем нажмите кнопку Подключиться.



Задания

Для выполнения лабораторной работы необходимо:

1) Проверить IP-адрес на принадлежность в списку "белый".
2) Настроить удаленный доступ к веб-интерфейсу интернет-центра.
3) Перенести зарегистрированное доменное имя с одного интернет-центра на другой.
4) Добавить VPN-подключение в ОС.
5) Оформить отчёт.
6) Ответить на контрольные вопросы.
7) Сделать вывод.

Контрольные вопросы:

1. Какой IP-адрес называется публичным IP-адресом?
2. Какие механизмы безопасности используются при реализации VPN-подключения?
3. Что такое «туннель» и в чем состоит принцип «туннелирования»?
4. В чем заключаются защитные функции виртуальных частных сетей?

Перечень основной литературы:

1. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. – М: РадиоСофт, 2010, - 255 с., 44 ил.

Перечень дополнительной литературы:

1 Сюваткин В.С. и др. WiMAX – технология беспроводной связи: основы теории , стандарты, применение / Под ред. Крылова В.В. – СПб.: БХВ-Петербург, 2005. – 368с.: ил.

2. Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильям», 2003. – 640 с.
3. Владимиров, А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / Андрей А. Владимиров, Константин В. Гавриленко, Андрей А. Михайловский; пер. с англ. АА. Слинкина. — М.: НТ Пресс, 2005. — 463, [1] с: ил.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ»
для студентов направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2025

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

− формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
− написание докладов;
− подготовка к семинарам, практическим и лабораторным работам, их оформление;
− составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
− выполнение учебно-исследовательских работ, проектная деятельность;
− подготовка практических разработок и рекомендаций по решению проблемной ситуации;
− выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
− компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
− выполнение курсовых работ (проектов) в рамках дисциплин;
− выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Защита информации в системах беспроводной связи» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (акад.)		
			СРС	Контактная работа с преподавателем	Всего
ПК-3(ИД-1ИД-2ИД-3)	Самостоятельное изучение литературы и источников	Собеседование	46,08	5,12	51,2
ПК-3(ИД-1ИД-2ИД-3)	Подготовка к лабораторным занятиям	Защита ЛР	9,72	1,08	10,8
ПК-3(ИД-1ИД-2ИД-3)	Написание реферата/доклада	Защита доклада	9	1	10
		Итого	64,8	7,2	72

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент

не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

- Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.
- Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;
● шрифт Times New Roman;
● кегль шрифта 14;
● межстрочное расстояние 1,5;
● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные	Проект не сдан.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.		поручения в групповом проекте.	

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа

до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

2. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. – М: РадиоСофт, 2010, - 255 с., 44 ил.

Дополнительная литература:

1. Сюваткин В.С. и др. WiMAX – технология беспроводной связи: основы теории , стандарты, применение / Под ред. Крылова В.В. – СПб.: БХВ-Петербург, 2005. – 368с.: ил.

2. Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильям», 2003. – 640 с.

3. Владимиров, А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / Андрей А. Владимиров, Константин В. Гавриленко, Андрей А. Михайловский; пер. с англ. АА. Слинкина. — М.: НТ Пресс, 2005. — 463, [1] с: ил.

Методическая литература:

1. Методические рекомендации по выполнению лабораторных работ по дисциплине "Защита информации в системах беспроводной связи"

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине "Защита информации в системах беспроводной связи"

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Цифровая грамотность и обработка больших данных»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.