Министерство цифрового развития, связи и массовых коммуникаций РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«___»_____2025 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ

Б1.В.24 Кибербезопасность и защита информации в сетях связи

Направление подготовки / специальность: **11.03.02 «Инфокоммуникационные технологии и системы связи»**

Направленность (профиль) /специализация: **Программирование и администрирование систем связи**

Форма обучения: **очная**

Год набора: *2026*

Разработчик:
доцент _____ / Е.С. Тарасов /
подпись

Оценочные средства обсуждены и утверждены на заседании кафедры инфокоммуникационных технологий и мобильной связи (ИТиМС)
Протокол от 27.11.2025 г. № 3
Заведующий кафедрой _____ /Н.В. Будылдина/
подпись

Екатеринбург, 2025

Министерство цифрового развития, связи и массовых коммуникаций РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«___»_____2025 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ

Б1.В.24 Кибербезопасность и защита информации в сетях связи

Направление подготовки / специальность: **11.03.02 «Инфокоммуникационные технологии и системы связи»**

Направленность (профиль) /специализация: **Программирование и администрирование систем связи**

Форма обучения: **очная**

Год набора: 2026

Разработчик:
доцент _____ / Е.С. Тарасов /
подпись

Оценочные средства обсуждены и утверждены на заседании кафедры инфокоммуникационных технологий и мобильной связи (ИТиМС)
Протокол от 27.11.2025 г. № 3
Заведующий кафедрой _____ /Н.В. Будылдина/
подпись

Екатеринбург, 2025

1. Перечень компетенций и индикаторов их достижения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенций	Этап	Предшествующие этапы (с указанием дисциплин/практик)
ПК-1 – Способен к проведению профилактических работ на оборудовании связи	ПК-1.3. Знает правила технической эксплуатации информационной безопасности при работе с телекоммуникационным оборудованием	4	Этап 1: Б1.В.21 Мультисервисные сети и протоколы Этап 2: Б1.В.22 Облачные платформы в телекоме Этап 3: Б1.В.23 Нормативно-правовая база профессиональной деятельности
ПК-5 – Способен выявлять и устранять сбои и отказы возникающих в сетевых устройствах информационно-коммуникационных системах	ПК-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств	1	

Форма промежуточной аттестации по дисциплине – экзамен

2. Показатели, критерии и шкалы оценивания компетенций

2.1. Показателем оценивания компетенций на этапе их формирования при изучении дисциплины является уровень их освоения.

Индикатор освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
ПК-1.3. Знает правила технической эксплуатации информационной безопасности при работе с телекоммуникационным оборудованием	Знает: - основные определения в области кибербезопасности; - основное законодательство РФ в области кибербезопасности; - виды вредоносного программного обеспечения; - виды сетевых атак; - методы защиты от различных сетевых атак; - политику	1. Выполнены все практические и лабораторные работы по дисциплине в соответствии с графиком. 2. Оформлены отчеты по практическим и лабораторным работам в соответствии с требованиям. 3. При защите лабораторных и практических работ может объяснить методы и технологии, используемые для их выполнения.

	информационной безопасности; - методы защиты сетевых устройств от несанкционированного доступа; - методы организации многоуровневой защиты сети от несанкционированного доступа; - принципы организации VPN; - протоколы сетей VPN; - виды и принцип работы различных вирусов; - основные виды и принцип работы антивирусных программ; Умеет: - определять уязвимости в сетях передачи данных; - выявлять сетевые атаки на сеть; - устранять последствия сетевых атак; - защищать сетевые устройства от несанкционированного доступа; - защищать сети передачи данных от несанкционированного доступа; - настраивать VPN; Владеет: навыками оформления технической документации по организации сетевой безопасности.	
ПК-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств	Знает: - основные определения в области кибербезопасности; - основное законодательство РФ в области кибербезопасности; - виды вредоносного программного	1. Выполнены все практические и лабораторные работы по дисциплине в соответствии с графиком. 2. Оформлены отчеты по практическим и лабораторным работам в соответствии с требованиям. 3. При защите лабораторных и практических работ может объяснить методы и технологии, используемые для их выполнения.

	обеспечения; - виды сетевых атак; - методы защиты от различных сетевых атак; - политику информационной безопасности; - методы защиты сетевых устройств от несанкционированного доступа; - методы организации многоуровневой защиты сети от несанкционированного доступа; - принципы организации VPN; - протоколы сетей VPN; - виды и принцип работы различных вирусов; - основные виды и принцип работы антивирусных программ; Умеет: - определять уязвимости в сетях передачи данных; - выявлять сетевые атаки на сеть; - устранять последствия сетевых атак; - защищать сетевые устройства от несанкционированного доступа; - защищать сети передачи данных от несанкционированного доступа; - настраивать VPN; Владеет: навыками оформления технической документации по организации сетевой безопасности.	

Шкала оценивания.

Экзамен

5-балльная шкала	Критерии оценки
Отлично	1. Самостоятельно и правильно ответил на поставленные теоретические вопросы экзаменационного билета. Уверенно, логично, последовательно и аргументировано излагает свой ответ. Может ответить на дополнительные вопросы. 2. Самостоятельно и правильно решил задачу экзаменационного билета. Уверенно и логично объясняет какие методы и технологии используются для ее решения.
Хорошо	1. Самостоятельно ответил на поставленные теоретические вопросы экзаменационного билета. Не уверенно отвечает на уточняющие и дополнительные вопросы. 2. Самостоятельно и правильно решил задачу экзаменационного билета. Уверенно и логично объясняет какие методы и технологии используются для ее решения.
Удовлетворительно	1. Самостоятельно ответил на поставленные теоретические вопросы экзаменационного билета. При этом допускает ошибки. Не уверенно или вообще не отвечает на уточняющие и дополнительные вопросы. 2. Решил задачу экзаменационного билета. При наличии ошибок, может исправить их за счет наводящих вопросов. Не уверенно объясняет какие методы и технологии используются для ее решения..
Неудовлетворительно	1. Не решена задача экзаменационного билета. 2. Решена задача, но не даны ответы на теоретические вопросы экзаменационного билета.

3. Методические материалы, определяющие процедуры оценивания по дисциплине

3.1. В ходе реализации дисциплины используются следующие формы и методы текущего контроля

Тема и/или раздел	Формы/методы текущего контроля успеваемости
ПК-1.3 Знает правила технической эксплуатации информационной безопасности при работе с телекоммуникационным оборудованием	
Раздел 1 Общие сведения о кибербезопасности	Экзамен
Раздел 2 Угрозы кибербезопасности	Экзамен
Раздел 3 Общие принципы защиты от сетевых атак	Экзамен
Раздел 4 Защита сетевых устройств от несанкционированного доступа	Экзамен Практические работы – зачет
Раздел 5 Аутентификация, авторизация и учет	Экзамен Лабораторная работа – зачет

Раздел 6 Защита сетей на канальном уровне	Экзамен Лабораторная работа – зачет
Раздел 7 Защита сетей на основе списков контроля доступа	Экзамен Лабораторная работа – зачет
Раздел 8 Основы криптографии	Экзамен
Раздел 9 Виртуальные частные сети	Экзамен Практические работы – зачет
Раздел 10 Организация сетевой безопасности на межсетевых экранах	Экзамен Лабораторная работа – зачет
Раздел 11 Защита оконечных устройств сетей	Экзамен Лабораторная работа – зачет
ПК-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств	
Раздел 1 Общие сведения о кибербезопасности	Экзамен
Раздел 2 Угрозы кибербезопасности	Экзамен
Раздел 3 Общие принципы защиты от сетевых атак	Экзамен
Раздел 4 Защита сетевых устройств от несанкционированного доступа	Экзамен Практические работы – зачет
Раздел 5 Аутентификация, авторизация и учет	Экзамен Лабораторная работа – зачет
Раздел 6 Защита сетей на канальном уровне	Экзамен Лабораторная работа – зачет
Раздел 7 Защита сетей на основе списков контроля доступа	Экзамен Лабораторная работа – зачет
Раздел 8 Основы криптографии	Экзамен
Раздел 9 Виртуальные частные сети	Экзамен Практические работы – зачет
Раздел 10 Организация сетевой безопасности на межсетевых экранах	Экзамен Лабораторная работа – зачет
Раздел 11 Защита оконечных устройств сетей	Экзамен Лабораторная работа – зачет

3.2. Типовые материалы текущего контроля успеваемости обучающихся

ПК-1.3 Знает правила технической эксплуатации информационной безопасности при работе с телекоммуникационным оборудованием

Типовое практическое задание:
по теме «*Изучение принципов управления конфигурацией и образами IOS*»

Задание:
1 Открыть файл ROMMON.
2 Ознакомиться с характеристикой корпоративной сети.

Компания состоит из двух офисов. Один находится в Екатеринбурге, другой в Первоуральске. В компании есть только то оборудование, которое показано на схеме. Другого нет.

ВНИМАНИЕ! Так как вы сотрудник офиса Первоуральска, то доступа к оборудованию Екатеринбурга у вас нет. Поэтому, ни каких действий совершать с оборудованием Екатеринбурга **НЕЛЬЗЯ!** Вы работаете исключительно с оборудованием Первоуральска. Однако, условно можно позвонить в офис Екатеринбурга и узнать настройки ихнего

оборудования. Это значит, что вы можете только посмотреть все необходимые настройки оборудования Екатеринбурга.

НЕЛЬЗЯ брать дополнительное обрудование и заменять существующее. По уловию запасного оборудрвания у вас нет. Все настройки необходимо выполнять исключительно с рабочего ноутбка Admin. Поэтому все скрины необхоимо сделать так, что бы было видно, что настройки ведутся с него.

3 Постановка проблемы.

В офисе Первоуральска была совершена внутренняя хакерская атака на оборудование. В результате вышло из строя оборудование. **НЕОБХОДИМО УЧЕСТЬ!** На маршрутизаторах должна стоять абсолютно одинаковая прошивка. Ваша задача: восстановить работу оборудования первого этажа в офисе Первоуральска так, что бы восстановить связь с офисом Екатеринбурга.

4 Требования к настройке.

4.1. На маршрутизаторе первого этажа необходимо выполнить следующие настройки:

1 Задать имя маршрутизатору в виде **вашей фамилии и инициалов**.

2 Задать доменное имя **Group<номер группы>.ru**. Вместо скобок указать свою группу.

3 Обеспечить доступ администратора из города Екатеринбурга к маршрутизатору по протоколу sshv2 с логином соответствующего **Вашему имени** и паролем **дата вашего рождния**. При успешной авторизации на маршрутизаторе, администратор должен ввести пароль **cisco** для доступа в привелигерованный режим.

4 Для связи с Екатеринбургом, нужна настройка, которую Вы не знаете, как выполнять. Однако, конфигурация с этой настройкой хранится на сервере tftp, под именем **Perv1.txt**.

5 Необходимо установить пароль на доступ к маршрутизатору по консольному порту. Логин для доступа **ваши инициалы**, пароль, **текущая дата**. При успешной авторизации на консольном порту, пользователь сразу должен попасть в привилегированный режим.

6 Все пароли должны хранится в зашифрованном виде.

4.2 На коммутаторе первого этажа были стерты все настройки. Они должны быть аналогичны настройкам коммутатора второго этажа. Необходимо восстановить эти настройки. После восстановления настроек обеспечить доступ администратору Екатеринбурга к коммутатору по защищенному соединению версии 2. Все коммутаторы должны взаимодествовать со своими маршрутизаторами, т. е. должен проходить пинг.

4.3 На маршрутизаторе второго этажа злоумышлинник изменил настройки и установил пароль на привилегированный режим. Необходимо:

1. Восстановить сетевое имя.

2. Обеспечить доступ администратору Екатеринбурга по защищенной удаленной связи с именем и паролем, аналогичным маршрутизатору Perv1.

3. Защитить привилегированный режим своим паролем.

4. Защитить доступ через консольный порт только по паролю **P@ssw0rd.**

4.4 Все устройства должны быть синхронизированы по времени.

5 Проверить, что бы все выполняемые задачи сети выполнялись.

6 Сделать резервные копии всех устройств Певоуральска.

Лабораторная работа по теме «*Исследование методов защиты сетевых устройств от несанкционированного доступа*»

Задание:

1 Скоммутировать сеть, показанную на рисунке 1.

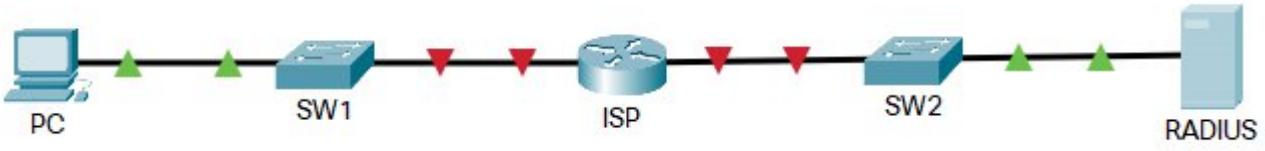

Рисунок 1 – Схема сети для настройки

По умолчанию на всех устройствах настроен удаленный доступ по протоколу Telnet.

2 На всех устройствах настроить сетевое имя, в соответствии со схемой на рисунке 1.

3 Настроить все межсетевые устройства так, что бы минимальная длина пароля была не менее пяти символов.

4 Настроить все межсетевые устройства так, что бы при двух не верно введенных паролей, в течение 1,5 минут, линия блокируется на одну минуту.

5 Настроить все межсетевые устройства так, что бы при бездействии в течении пяти минут, устройство завершало сеанс в привилегированном режиме.

6 Настроить все межсетевые устройства так, что бы все пароли хранились в зашифрованном виде.

7. Защитить консольные линии всех межсетевых устройств от несанкционированного доступа. **ВНИМАНИЕ!** Пароли должны быть надежными!

7.1 Коммутаторы с помощью пароля, который должен соответствовать вашему имени.

7.2 Маршрутизатор с помощью логина, который должен соответствовать вашим инициалам и паролем, который должен соответствовать вашей фамилии.

8 Защитить VTY всех межсетевых устройств от несанкционированного доступа. **ВНИМАНИЕ!** Пароли должны быть надежными!

8.1 Коммутаторы, используя модель AAA и локальную базу учетных записей. В качестве логина использовать вашу фамилию и инициалы, пароль придумать самостоятельно, который должен соответствовать всем требованиям к безопасности.

8.2 Доступ к маршрутизатору должен осуществляться с использованием RADIUS сервера. Логин для доступа root, пароль p@ssw0rd2022!. Ключевое слово

9 Защитить привилегированный режим всех межсетевых устройств от несанкционированного доступа. Пароль придумать самостоятельно, который должен соответствовать всем требованиям к безопасности. Пароль не должен совпадать с паролем в пункте 8.1. Пароль должен шифроваться 9 типом.

Типовое задание для самостоятельной работы:

1. Изучение конспекта лекций и литературы
2. Подготовка отчета по практической работе
3. Подготовка отчета по лабораторной работе
4. Подготовка к экзамену.

ПК-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств

Типовое практическое задание:

по теме «*Настройка VPN типа Site-to-Site»*

Задание:

Компания имеет два филиала, в Москве и Санкт-Петербурге. Схема сети показана на рисунке 1.

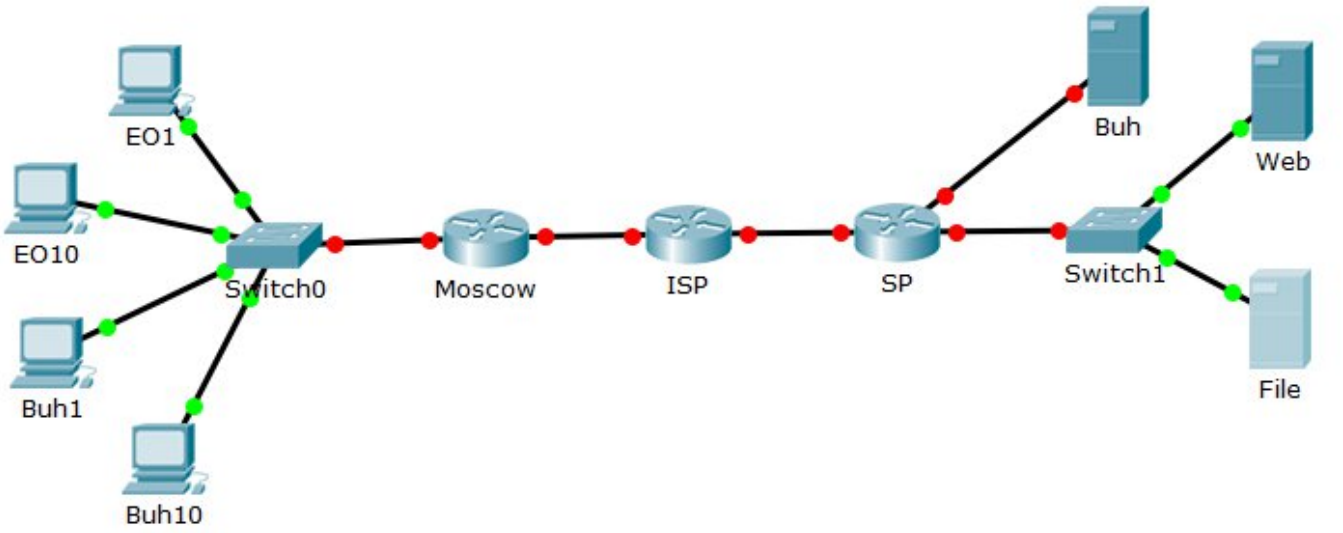

Рисунок 1 – Схема организации связи сети компании

Филиалы соединяются между собой через сеть Internet, роль которой играет маршрутизатор ISP. В Санкт-Петербурге установлены серверы. Отделы, которые должны пользоваться этими серверами, находятся в Москве. К серверу Buh должны иметь только компьютеры бухгалтерии по защищенному каналу. К Web серверу могут иметь все пользователи по не защищенному каналу. К File серверу должны иметь доступ все корпоративные пользователи по защищенному каналу. Оба филиала имеют только один публичный IP-адрес от провайдера. Необходимо учитывать, что внутри Московского филиала должна быть связь между отделами.

Настроить сетевые имена маршрутизаторам.

Лабораторная работа по теме «*Настройка сетевой безопасности с помощью функции Port Security*»

Задание:

1 Скоммутировать сеть, показанную на рисунке 1.

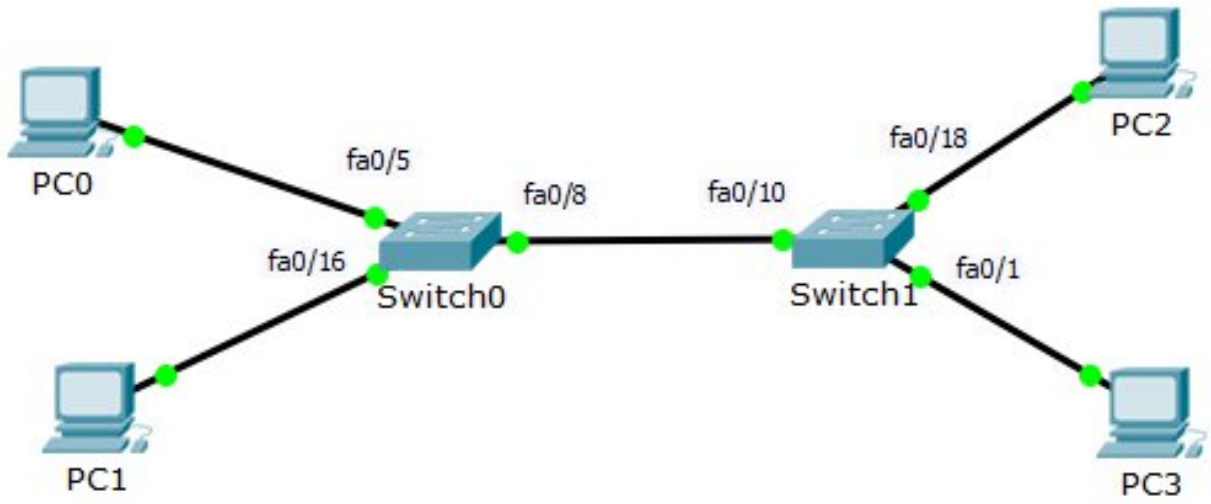

Рисунок 1 – Сеть для настройки

2 Через порт fa0/10 могли работать только PC0 и PC1. При нарушении режима безопасности должны формироваться сообщения в журнал логов, но порт отключаться не должен.

3 Через порт fa0/8 должны работать не более трех компьютеров, два из которых обязательно PC3 и PC4. При нарушении режима безопасности должен только блокироваться трафик.

4 Через порты fa0/1, 5, 16, 18 должны работать только соответствующие PC. При нарушении режима безопасности эти порты должны блокироваться.

5 Настроить порты fa0/5 и 16 так, что бы при отсутствии активности на этих портах в течение 5 минут, защита удалялась

6 Настроить порты fa0/1 и 18 так, что бы защита удалялась через 15 минут.

7 На Switch0 предусмотреть два порта через которые смогут подключиться к сети не более трех компьютеров.

8 На Switch1 предусмотреть три порта через которые смогут подключиться к сети не более двух компьютеров.

9 Все порты коммутаторов должны быть защищены от несанкционированного доступа.

10 Проверить правильность настройки коммутаторов.

Типовое задание для самостоятельной работы:

1. Изучение конспекта лекций и литературы
2. Подготовка отчета по практической работе
3. Подготовка отчета по лабораторной работе
4. Подготовка к экзамену.

3.3. Типовые материалы для проведения промежуточной аттестации обучающихся

ПК-1.3 Знает правила технической эксплуатации информационной безопасности при работе с телекоммуникационным оборудованием

Типовые вопросы и задания к экзамену:

1. Основные понятия в области безопасности. Виды хакеров. Их особенности.

2. Понятие вредоносного программного обеспечения. Группы вредоносных программ и их действие: рекламные, шпионские, трояны, вымогатели.

3. Понятие вредоносного программного обеспечения. Группы вредоносных программ и их действие: черви, вирусы, боты, логические бомбы.

4. Понятие политики безопасности. Перечислить разделы, которые могут входить в нее. Пояснить состав разделов: физической безопасности, эксплуатации электронных устройств, управления доступом.

5. Понятие политики безопасности. Перечислить разделы, которые могут входить в нее. Пояснить состав разделов: сетевой безопасности, программного обеспечения, парольной защиты.

6. Понятие политики безопасности. Перечислить разделы, которые могут входить в нее. Пояснить состав разделов: антивирусной защиты, использования Интернета, электронной поты, внешних носителей, резервного копирования.

7. Методы защиты сетевых устройств от несанкционированного доступа. Требования к паролям. Сравнительная характеристика протоколов Telnet и ssh.

8. Назначение протокола RADIUS. Его характеристики. Роли устройств при работе протокола RADIUS.

9. Назначение и принцип функционирования таблицы адресов. Атака на таблицу адресов. Методы защиты сетей от данного вида атак.

10. Назначение и процедурная характеристика протокола DHCP. Виды атак на DHCP сервер. Методы защиты от данного вида атак.

11. Назначение и процедурные характеристики протокола ARP. Атаки на протокол ARP. Методы защиты от данного вида атак.

12. Пояснить принцип работы протокола STP.Виды атак на протокол STP. Методы защиты от данного вида атак.

13. Понятие сетевой атаки. Типы сетевых атак: сниффинг, IP-спуффинг, DoS, парольная. Их реализация. Методы защиты.

14. Понятие сетевой атаки. Типы сетевых атак: человек между, приложений, сетевая разведка, злоупотребление доверием, вирусы и трояны. Их реализация. Методы защиты.

15. Понятие ACL. Их назначение и классификация. Пояснить принцип фильтрации трафика. Понятие шаблонная маска. Принцип ее определения.

ПК-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств

Типовые вопросы и задания к экзамену:

1. Понятие VPN. Преимущества их использования. Типы VPN, их сравнительная характеристика. Протоколы VPN: PPTP, SSTP. Их особенности.

2. Понятие VPN. Преимущества их использования. Типы VPN, их сравнительная характеристика. Протокол VPN: IPsec. Его характеристика, область использования.

3. Понятие VPN. Преимущества их использования. Типы VPN, их сравнительная характеристика. Протоколы VPN: Open VPN, Wire Guard. Их особенности.

4. Назначение стека протоколов IPsec. Его характеристика и функции. Принцип обеспечение конфиденциальности данных.

5. Назначение стека протоколов IPsec. Его характеристика и функции. Принцип обеспечение целостности данных.

6. Назначение стека протоколов IPsec. Его характеристика и функции. Принцип аутентификации устройств методом PSK.

7. Назначение стека протоколов IPsec. Его характеристика и функции. Принцип аутентификации устройств методом RSA.

8. Назначение стека протоколов IPsec. Его характеристика и функции. Сравнительная характеристика групп обмена ключами по алгоритму DH. Принцип формирования и обмена ключами.

9. Назначение стека протоколов IPsec. Его характеристика и функции. Состав стека и назначение протоколов. Принцип работы протокола AH. Формат пакета.

10. Назначение стека протоколов IPsec. Его характеристика и функции. Состав стека и назначение протоколов. Принцип работы протокола ESP. Формат пакета. Режимы работы.

11. Назначение стека протоколов IPsec. Его характеристика и функции. Состав стека и назначение протоколов. Процедура установления туннеля между устройствами.

12. Понятие вирусов. Их классификация. Особенности действия различных типов вирусов.

13. Понятие вирусов. Их классификация по разрушительным способностям, и способу заражения. Признаки наличия вирусов на компьютере.

14. Понятие вирусов. Их классификация по среде обитания и и принципу функционирования. Основные правила по защите компьютеров от проникновения вирусов.

15. Назначение антивирусных программ. Требования, предъявляемые к этим программам. Группы антивирусных программ: детекторы, доктора, сторожа. Их работа и область применения.

16. Назначение антивирусных программ. Требования, предъявляемые к этим программам. Группы антивирусных программ: сторожа, ревизоры, вакцинаторы. Их работа и область применения.

3.4. Методические материалы проведения текущего контроля и промежуточной аттестации обучающихся

Перечень методических материалов для подготовки к текущему контролю и промежуточной аттестации:

1. Методические указания к выполнению практических работ по дисциплине «Кибербезопасность и защита информации в сетях связи». –URL: http://aup.uisi.ru/5079773/
2. Методические указания к выполнению лабораторных работ по дисциплине «Кибербезопасность и защита информации в сетях связи». –URL: http://aup.uisi.ru/5079773/