Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
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
_____ Минина Е.А.
«__» _____ 2023 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ

Б1.В.24 Защита информации от несанкционированного доступа

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

Направленность (профиль) /специализация: **Инфокоммуникационные технологии в услугах связи**

Форма обучения: **очная**

Год набора: 2024

Разработчик (-и):
доцент _____ / Е.С. Тарасов /
подпись

Оценочные средства обсуждены и утверждены на заседании инфокоммуникационных технологий и мобильной связи (ИТиМС)
Протокол от 28.11.2023 г. № 3
Заведующий кафедрой _____ / Н.В. Будылдина /
подпись

Екатеринбург, 2023

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
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
_____Минина Е.А.
«____» _____2023 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
Б1.В.24 Защита информации от несанкционированного доступа

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

Направленность (профиль) /специализация: **Инфокоммуникационные технологии в услугах связи**

Форма обучения: **очная**

Год набора: 2024

Разработчик (-и):
доцент _____ / Е.С. Тарасов /
подпись

Оценочные средства обсуждены и утверждены на заседании инфокоммуникационных технологий и мобильной связи (ИТиМС)
Протокол от 28.11.2023 г. № 3
Заведующий кафедрой _____ / Н.В. Будылдина /
подпись

Екатеринбург, 2023

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-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	4	Этап 1 Б1.В.11, Сетевые технологии высокоскоростной передачи данных, Б1.В.14 Сети и системы радиосвязи. Этап 2 Б1.В.15 Администрирование в инфокоммуникационных системах, Б1.В.17Архитектура и программное обеспечение сетевых инфокоммуникационных устройств. Этап 3 Б1.В.22 Теория телетрафика, Б1.В.ДВ.02.01Проектирование локальных сетей.

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-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств	Знает: -виды сетевых угроз и методы их реализации; - методы криптографичекой защиты информации; - методы защиты от сетевых угроз на разных уровнях эталонной модели; - методы организации виртуальных частных сетей; - методы защиты информации на оконечном оборудовании. Умеет:	1. Выполнены все лабораторные и практические работы по дисциплине в соответствии с графиком. 2. Оформлены отчеты по лабораторным и практическим работам в соответствии с требованиям. 3. При защите лабораторных работ обосновывает необходимость выполнения всех настроек. 4. При защите практических работ обосновывает выбранные технические решения для организации защиты сетей.

	- настраивать функцию Port Security; - создавать Access Control List; -защищать сеть передачи данных с помощью межсетевого экрана; - защищать сетевое оборудование от несанкционированного доступа; - создавать VPN соединения. Владеет: - навыками решения производственных задач по защите сетевой безопасности.	

Шкала оценивания.

5-балльная шкала	Критерии оценки
«Отлично»	Самостоятельно и правильно ответил на поставленные вопросы экзаменационного билета. Уверенно, логично, последовательно и аргументировано излагает свой ответ. Может ответить на дополнительные вопросы.
«Хорошо»	Самостоятельно ответил на поставленные вопросы экзаменационного билета. Не уверенно отвечает на уточняющие и дополнительные вопросы.
«Удовлетворительно»	Самостоятельно ответил на поставленные вопросы экзаменационного билета. При этом допускает ошибки. Не уверенно или вообще не отвечает на уточняющие и дополнительные вопросы.
«Неудовлетворительно»	Не ответил хотя бы на один вопрос 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-5.4 Умеет анализировать состояние и выявлять сбои, устранять последствия сбоев и отказов сетевых устройств	
Раздел 1 Сетевые угрозы	Экзамен
Раздел 2 Общие принципы защиты от сетевых атак	Экзамен
Раздел 3 Защита сетевых устройств от несанкционированного доступа	Экзамен Практическая работа
Раздел 4 Аутентификация, авторизация и учет	Экзамен

	Лабораторная работа – зачет
Раздел 5 Защита сетей на канальном уровне	Экзамен Лабораторная работа
Раздел 6 Защита сетей на основе списков контроля доступа	Экзамен Лабораторная работа
Раздел 7 Виртуальные частные сети	Экзамен Лабораторная работа
Раздел 8 Организация сетевой безопасности на межсетевых экранах	Экзамен Лабораторная работа Практическая работа
Раздел 9 Защита оконечных устройств сетей	Экзамен

3.2. Типовые материалы текущего контроля успеваемости обучающихся

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

Пример задания на практическое занятие

1 Цель работы:

1.1 Изучить порядок копирования и восстановления образов операционной системы IOS Cisco и пользовательской конфигурации.

2 Задание:

2.1 Открыть файл ROMMON.

2.2 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.

2.3 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.

2.4 Требования к настройке.

2.4.1. На маршрутизаторе первого этажа необходимо выполнить следующие настройки:

- Задать имя маршрутизатору в виде **вашей фамилии и инициалов**.
- Задать доменное имя **Group<номер группы>.ru**. Вместо скобок указать свою группу.
- 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.

- 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**.

- 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.

- Все пароли должны хранится в зашифрованном виде.

2.4.2 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.

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

- Восстановить сетевое имя.

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

- Защитить привилегированный режим своим паролем.

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

2.4.4 Все устройства должны быть синхронизированы по времени.

2.5 Проверить, что бы все выполняемые задачи сети выполнялись.

2.6 Сделать резервные копии всех устройств Первоуральска.

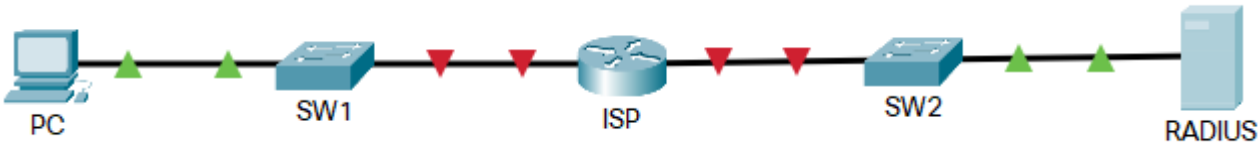
Пример задания на лабораторную работу

1 Цель работы:

1.1 Исследовать принципы защиты сетевых устройств от несанкционированного доступа.

2 Задание:

2.1 Скоммутировать сеть, показанную на рисунке.



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

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

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

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

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

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

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

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

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

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

2.8.1 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.

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

2.9 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 2.8.1. Пароль должен шифроваться 9 типом.

3.3. Типовые материалы для проведения промежуточной аттестации обучающихся

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. Назначение VLAN. Преимущества их создания. Виды VLAN. Формат кадра протокола IEEE 802.1Q. Виды настраиваемых портов. Порядок продвижения немаркированного кадра через коммутатор с настроенными VLAN.
14. Назначение VLAN. Преимущества их создания. Виды VLAN. Формат кадра протокола IEEE 802.1Q. Виды настраиваемых портов. Порядок продвижения маркированного кадра через коммутатор с настроенными VLAN.

15. Назначение VLAN. Преимущества их создания. Назначение протокола GVRP. Формат кадра, виды сообщений. Процедура динамического создания VLAN.

16. Назначение VLAN. Преимущества их создания. Назначение протокола GVRP. Формат кадра, виды сообщений. Процедура динамического удаления VLAN.

17. Назначение VLAN. Преимущества их создания. Понятие Q-in-Q VLAN. Область ее использования. Формат кадра. Особенности реализации Port Based. Процедура передачи кадра в сетях с Q-in-Q VLAN.

18. Назначение VLAN. Преимущества их создания. Понятие Q-in-Q VLAN. Область ее использования. Формат кадра. Особенности реализации Selective. Процедура передачи кадра в сетях с Q-in-Q VLAN.

19. Назначение VLAN. Преимущества их создания. Виды VLAN. Порядок продвижения кадра через коммутатор с настроенными VLAN. Виды атак на VLAN. Методы защиты от данного вида атак.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Банк контрольных вопросов, заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации находится в учебно-методическом комплексе дисциплины и/или представлен в электронной информационно-образовательной среде по URI: http://www.aup.uisi.ru/.

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 лабораторных работ по дисциплине «Защита информации от несанкционированного доступа». –URL: https://aup.uisi.ru/3558494/?offset=10.
2. Методические указания к выполнению практических работ по дисциплине «Защита информации от несанкционированного доступа». –URL: https://aup.uisi.ru/3558494/?offset=10.