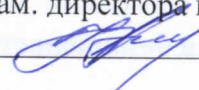


МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УР

 Н.А. Андреева

« 31 » 03 2025г.

Б1.В.15 Сетевая безопасность

рабочая программа дисциплины

Кафедра **Инфокоммуникационных технологий и систем связи**

Направление подготовки **11.03.02 Инфокоммуникационные технологии и системы связи**

Профиль **Инфокоммуникационные системы и сети**

Формы обучения **Защищенные инфокоммуникационные системы
очная, заочная, очно-заочная**

Распределение часов дисциплины по семестрам (для очной и очно-заочной форм обучения (ОФО и ОЗФО)), курсам (для заочной формы обучения (ЗФО))

Вид учебной работы	ОФО		ЗФО		ОЗФО	
	ЗЕ	часов/ семестр	ЗЕ	часов/ курс	ЗЕ	часов/ семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/8	4	36/4 108/5	4	144/9
Контактная работа, в том числе (по семестрам, курсам):		50/8		2/4 22/5		24/9
Лекции		10/8		2/4 6/5		8/9
Лабораторные работы		20/8		8/5		8/9
Практические занятия		20/8		8/5		8/9
Семинарские занятия						
Самостоятельная работа обучающихся		58/8		34/4 77/5		84/9
Контроль		36/8		9/5		36/9
Число контрольных работ (по семестрам, курсам)						
Число КР (по семестрам, курсам)						
Число КП (по семестрам, курсам)						
Число зачетов (с разбивкой по семестрам, курсам)						
Число зачетов с оценкой (с разбивкой по семестрам, курсам)						
Число экзаменов (с разбивкой по семестрам, курсам)		1/8		1/5		1/9

Программу составил(ли):

Доцент кафедры ИТСС, к.т.н., доцент Манин А.А.

Рабочая программа дисциплины

«Сетевая безопасность»

Разработана в соответствии с ФГОС ВО

направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

Составлена на основании учебного(ных) плана(нов)

направления 11.03.02 Инфокоммуникационные технологии и системы связи, профиля(лей) «Инфокоммуникационные системы и сети», «Защищенные инфокоммуникационные системы», одобренных) Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024 г., и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «22» 04 2024 г. № 9

Зав. кафедрой  В.И.Юхнов

1. Цели изучения дисциплины

Целями изучения дисциплины «Сетевая безопасность» являются овладение совокупностью технологий, способов, средств и методов защиты информации, циркулирующей в сетях связи, обеспечение ее целостности, конфиденциальности и доступности.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать следующие профессиональные задачи в соответствии с технологическим видом деятельности.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ПК-3: Способен выполнять работы по администрированию процесса управления безопасностью сетевых устройств и программного обеспечения	
Знать:	
- понятия целостность, конфиденциальность, доступность как основных характеристик защищенности информации; - модели политик информационной безопасности в сетях связи; - средства обеспечения защищенного доступа к сетевому оборудованию; - протоколы защищенного информационного обмена в сетях связи; - основные способы организации безопасного соединения через незащищенные общедоступные сети. - принципы функционирования аппаратно-программных средств защиты информации в сетях связи; - принципы внедрения средств защиты информации в сети связи; - принципы мониторинга инцидентов с использованием аппаратно-программных средств защиты информации в сетях связи.	
Уметь:	
- классифицировать и оценивать угрозы информационной безопасности в сетях связи; - проводить работы по администрированию средств защиты информации в сетях связи; - использовать механизмы аутентификации и авторизации в сетях связи; - конфигурировать встроенные в сетевое оборудование средства защиты; - проводить работы по разграничению прав доступа пользователей к сетевым ресурсам; - проводить работы по конфигурированию и администрированию аппаратно-программных средств защиты информации в сетях связи.	
Владеть:	
- основными понятиями, связанными с обеспечением безопасности в сетях связи; - навыками работы по конфигурированию средств защиты сетей связи; - навыками конфигурирования защищенного удаленного доступа; - навыками конфигурирования средств аутентификации; - навыками конфигурирования аппаратно-программных средств межсетевого экранирования; - навыками конфигурирования аппаратно-программных средств для организации виртуальных частных сетей.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.24 Основы информационной безопасности
2	Б1.В.01 Общая теория связи
3	Б1.В.04 Сетевые технологии
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.О.03(Пд) Производственная практика (преддипломная)
2	Б3.01 Выполнение и защита выпускной квалификационной работы

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 50 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 4, Семестр 8					
Модуль 1. Методы и средства защиты элементов сетей от НСД (6 Лек+12ЛР+12ПЗ) часов контактной работы 30 часов СР					
1.1	Лекция 1. МОДЕЛИ ПОЛИТИК БЕЗОПАСНОСТИ 1. Общие понятия. 2. Дискреционная модель. 3. Мандатная модель. 4. Ролевая модель. 5. Результативная кибербезопасность	Лек.	2	ПК-3	Л 3.1
1.2	Лекция 2. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ 1. Защита консольного доступа. 2. Протоколы удаленного доступа к сетевому оборудованию. 3. Защита удаленного доступа. 4. Протоколы RADIUS и TACACS+. 5. Принципы конфигурирования маршрутизаторов для работы с протоколом TACACS+. 6. Логирование сетевых событий.	Лек.	2	ПК-3	Л 1.1
1.3	Практическое занятие 1 Конфигурирование защиты консольного доступа	ПЗ	4	ПК-3	Л 3.1
1.4	Практическое занятие 2 Конфигурирование защиты удаленного доступа	ПЗ	4	ПК-3	Л 3.1
1.5	Практическое занятие 3 Конфигурирование защиты удаленного доступа с использованием AAA- и Syslog-серверов	ПЗ	4	ПК-3	Л 3.1
1.6	Лекция 3. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ 1. Определение и классификация межсетевых экранов. 2. Межсетевое экранирование с пакетной фильтрацией. 3. Межсетевое экранирование с сохранением состояний. 4. Зональные межсетевые экраны (Zone-Based Policy Firewall). 5. Межсетевые экраны следующего поколения (NGFW) 6. Структура сети с NGFW.	Лек.	2	ПК-3	Л 1.1
1.7	Лабораторная работа 1. Исследование свойств межсетевого экрана с пакетной фильтрацией	ЛР	4	ПК-3	Л 3.1
1.8	Лабораторная работа 2. Исследование свойств межсетевого экрана с сохранением состояний	ЛР	4	ПК-3	Л 3.1
1.9	Лабораторная работа 3. Исследование свойств межсетевого экрана ZBFW	ЛР	4	ПК-3	Л 3.1
1.10	Требования нормативных документов и технических регламентов к защищенным сетям связи	СР	6	ПК-3	Л 1.1
1.11	Технические характеристики аппаратных межсетевых экранов различных производителей	СР	8	ПК-3	Л 1.1
1.12	Обеспечение защиты беспроводного сетевого оборудования	СР	8	ПК-3	Л 1.2
1.13	Механизмы комплексной защиты сетей электросвязи	СР	8	ПК-3	Л 2.1
Модуль 2 Защита корпоративных сетей от НСД (4Лек+8ЛР+8ПЗ) часов контактной работы 28 часов СР					
2.1	Лекция 4. ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ЛОКАЛЬНЫХ И КОРПОРАТИВНЫХ СЕТЕЙ	Лек.	2	ПК-3	Л 3.1

	1. Уровни сетевой защиты. 2. Технология трансляции сетевых адресов (NAT). 3. Защита от атак на VLAN. 4. Защита от атак на протокол STP. 5. Использование функции Port Security. 6. Защита от атак на протоколы DHCP и ARP.				
2.2	Лекция 5. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) 1. Технологии туннелирования. Протокол GRE. 2. Архитектура IPSec. 3. Протокол AH. 4. Протокол ESP. 5. Принципы конфигурирования VPN IPSec.	Лек.	2	ПК-3	Л 1.2
2.3	Практическое занятие 4. Построение локальной сети с комплексной защитой	ПЗ	4	ПК-3	Л 3.1
2.4	Практическое занятие 5 Конфигурирование Site-to-Site VPN	ПЗ	4	ПК-3	Л 3.1
2.5	Лабораторная работа 4. Исследование повышения доступности сети с виртуальным маршрутизатором	ЛР	4	ПК-3	Л 3.1
2.6	Лабораторная работа 5. Исследование VPN туннеля	ЛР	4	ПК-3	Л 3.1
2.7	Механизмы защиты корпоративной сети от компьютерных вирусов	СР	10	ПК-3	Л 1.2
2.8	Области применения технологий VPN второго уровня	СР	10	ПК-3	Л 1.2
2.9	Организационные мероприятия по комплексной защите корпоративной сети	СР	8	ПК-3	Л 1.2
	Экзамен		36	ПК-3	
Итого – 144 часа					

4.2 Заочная форма обучения, 5 лет (всего 144 часа, 24 часа контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 5, Семестр 9					
Модуль 1. Методы и средства защиты элементов сетей от НСД 10 (2 Лек+4ЛР+4ПЗ) часов контактной работы 54 часа СР					
1.1	МОДЕЛИ ПОЛИТИК БЕЗОПАСНОСТИ 1. Общие понятия. 2. Дискреционная модель. 3. Мандатная модель. 4. Ролевая модель. 5. Результативная кибербезопасность	СР	4	ПК-3	Л 3.1
1.2	Лекция 1. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ 1. Защита консольного доступа. 2. Протоколы удаленного доступа к сетевому оборудованию. 3. Защита удаленного доступа. 4. Использование AAA-сервера для защиты удаленного доступа. 5. Логирование сетевых событий.	Лек.	2	ПК-3	Л 1.1
1.3	Протоколы RADIUS и TACACS+. Принципы конфигурирования маршрутизаторов для работы с протоколом TACACS+.	СР	4	ПК-3	Л 3.1
1.4	Практическое занятие 1 Конфигурирование защиты консольного и удаленного доступа	ПЗ	4	ПК-3	Л 3.1
1.5	МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ 1. Определение и классификация межсетевых экранов. 2. Межсетевое экранирование с пакетной фильтрацией.	СР	10	ПК-3	Л 1.1

	3. Межсетевое экранирование с сохранением состояний. 4. Зональные межсетевые экраны (Zone-Based Policy Firewall). 5. Межсетевые экраны следующего поколения (NGFW) 6. Структура сети с NGFW.				
1.6	Лабораторная работа 1. Исследование свойств межсетевых экранов	ЛР	4	ПК-3	Л 3.1
	Свойства и характеристики межсетевых экранов с пакетной фильтрацией, с сохранением состояний (SPI), экранов ZSPFW	СР	6	ПК-3	Л 3.1
1.7	Требования нормативных документов и технических регламентов к защищенным сетям связи	СР	6	ПК-3	Л 1.2
1.8	Технические характеристики аппаратных межсетевых экранов различных производителей	СР	8	ПК-3	Л 1.1
1.9	Обеспечение защиты беспроводного сетевого оборудования	СР	8	ПК-3	Л 1.2
1.10	Механизмы комплексной защиты сетей электросвязи	СР	8	ПК-3	Л 1.2
Модуль 2 Защита корпоративных сетей от НСД 14 (6Лек+4ЛР+4ПЗ) часов контактной работы 57 часов СР					
2.1	Лекция 2. ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ЛОКАЛЬНЫХ И КОРПОРАТИВНЫХ СЕТЕЙ 1. Уровни сетевой защиты. 2. Технология трансляции сетевых адресов (NAT). 3. Защита от атак на VLAN. 4. Защита от атак на протокол STP. 5. Использование функции Port Security. 6. Защита от атак на протоколы DHCP и ARP.	Лек.	4	ПК-3	Л 3.1
2.2	Лекция 3. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) 1. Технологии туннелирования. Протокол GRE. 2. Архитектура IPSec. 3. Протокол AH. 4. Протокол ESP. 5. Принципы конфигурирования VPN IPSec.	Лек.	2	ПК-3	Л 1.2
2.3	Практическое занятие 2. Построение локальной сети с комплексной защитой	ПЗ	4	ПК-3	Л 3.1
2.4	Особенности конфигурирования Site-to-Site VPN	СР	12	ПК-3	Л 3.1
2.5	Лабораторная работа 2. Исследование повышения доступности сети с виртуальным маршрутизатором	ЛР	4	ПК-3	Л 3.1
2.6	Свойства и особенности VPN туннелей IPSec	СР	10	ПК-3	Л 1.2
2.7	Механизмы защиты корпоративной сети от компьютерных вирусов	СР	10	ПК-3	Л 1.2
2.8	Области применения технологий VPN второго и третьего уровней	СР	14	ПК-3	Л 1.2
2.9	Организационные мероприятия по комплексной защите корпоративной сети	СР	11	ПК-3	Л 1.2
	Экзамен		9	ПК-3	
Итого – 144 часа					

4.3 Очно-заочная форма обучения 5 лет (всего 144 часа, 24 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМНО
1	2	3	4	5	6
Курс 5, Семестр 9					
Модуль 1. Методы и средства защиты элементов сетей от НСД 12 (4 Лек+4ЛР+4ПЗ) часов контактной работы 48 часов СР					

1.1	МОДЕЛИ ПОЛИТИК БЕЗОПАСНОСТИ 1. Общие понятия. 2. Дискреционная модель. 3. Мандатная модель. 4. Ролевая модель. 5. Результативная кибербезопасность	СР	6	ПК-3	Л 3.1
1.2	Лекция 1. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ 1. Защита консольного доступа. 2. Протоколы удаленного доступа к сетевому оборудованию. 3. Защита удаленного доступа. 4. Использование AAA-сервера для защиты удаленного доступа. 5. Логирование сетевых событий.	Лек.	2	ПК-3	Л 1.1
1.3	Протоколы RADIUS и TACACS+. Принципы конфигурирования маршрутизаторов для работы с протоколом TACACS+.	СР	6	ПК-3	Л 3.1
1.4	Практическое занятие 1 Конфигурирование защиты консольного и удаленного доступа	ПЗ	4	ПК-3	Л 3.1
1.5	МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ 1. Определение и классификация межсетевых экранов. 2. Межсетевое экранирование с пакетной фильтрацией. 3. Межсетевое экранирование с сохранением состояний. 4. Зональные межсетевые экраны (Zone-Based Policy Firewall). 5. Межсетевые экраны следующего поколения (NGFW) 6. Структура сети с NGFW.	СР	6	ПК-3	Л 1.1
1.6	Лабораторная работа 1. Исследование свойств межсетевых экранов	ЛР	4	ПК-3	Л 3.1
	Свойства и характеристики межсетевых экранов с пакетной фильтрацией, с сохранением состояний (SPI), экранов ZSPFW	СР	6	ПК-3	Л 3.1
1.7	Требования нормативных документов и технических регламентов к защищенным сетям связи	СР	6	ПК-3	Л 1.2
1.8	Технические характеристики аппаратных межсетевых экранов различных производителей	СР	6	ПК-3	Л 1.1
1.9	Обеспечение защиты беспроводного сетевого оборудования	СР	6	ПК-3	Л 1.2
1.10	Механизмы комплексной защиты сетей электросвязи	СР	6	ПК-3	Л 1.2
Модуль 2 Защита корпоративных сетей от НСД 12 (4Лек+4ЛР+4ПЗ) часов контактной работы 36 часов СР					
2.1	Лекция 2. ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ЛОКАЛЬНЫХ И КОРПОРАТИВНЫХ СЕТЕЙ 1. Уровни сетевой защиты. 2. Технология трансляции сетевых адресов (NAT). 3. Защита от атак на VLAN. 4. Защита от атак на протокол STP. 5. Использование функции Port Security. 6. Защита от атак на протоколы DHCP и ARP.	Лек.	4	ПК-3	Л 3.1
2.2	Лекция 3. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) 1. Технологии туннелирования. Протокол GRE. 2. Архитектура IPSec. 3. Протокол AH. 4. Протокол ESP. 5. Принципы конфигурирования VPN IPSec.	Лек.	2	ПК-3	Л 1.2
2.3	Практическое занятие 2. Построение локальной сети с комплексной защитой	ПЗ	4	ПК-3	Л 3.1
2.4	Особенности конфигурирования Site-to-Site VPN	СР	6	ПК-3	Л 3.1
2.5	Лабораторная работа 2. Исследование повышения доступности сети с виртуальным маршрутизатором	ЛР	4	ПК-3	Л 3.1

2.6	Свойства и особенности VPN туннелей IPSec	СР	6	ПК-3	Л 1.2
2.7	Механизмы защиты корпоративной сети от компьютерных вирусов	СР	8	ПК-3	Л 1.2
2.8	Области применения технологий VPN второго и третьего уровней	СР	8	ПК-3	Л 1.2
2.9	Организационные мероприятия по комплексной защите корпоративной сети	СР	8	ПК-3	Л 1.2
	Экзамен		36	ПК-3	
Итого – 144 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Милославская Н.Г., Толстой А.И.	Межсетевые экраны. Учебное пособие для вузов.	М.: Горячая линия – Телеком, 2024	Э1
Л1.2	Духан Е.И., Киллеров А.С., Синадский Н.И.	Методы и средства криптографической защиты информации	М.: Горячая линия – Телеком, 2024	Э2
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Шелухин О.И., Сакалема Д.Ж., Филинова А.С.	Обнаружение вторжений в компьютерные сети [сетевые аномалии]	М.: Горячая линия – Телеком, 2024	Э3
5.1.3 Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Манин А.А.	Методы и средства защиты компьютерной информации. Учебное пособие.	Ростов-на-Дону : Полиграфический центр СКФ МТУСИ, 2019	Э4
5.2 Электронные образовательные ресурсы				
Э1	https://elib.mtuci.ru/view.php?book_id=34676			
Э2	https://elib.mtuci.ru/view.php?book_id=34653			
Э3	https://elib.mtuci.ru/view.php?book_id=3598			
Э4	https://elib.mtuci.ru/view.php?book_id=170036			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.4 Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства				
П.1	ОС Windows			
П.2	ОС Linux			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком),

	экраном
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы	
Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.	

8. Методические рекомендации по освоению дисциплины	
Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.	

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.).

Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитав задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.В15 Сетевая безопасность» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи

Профиль: **Инфокоммуникационные системы и сети**
Защищенные инфокоммуникационные системы

Форма обучения: очная, заочная, очно-заочная

(Возможны следующие варианты):

- а) Рабочая программа действует без изменений.
- б) В рабочую программу вносятся следующие изменения:
 - 1)
 - 2)
 - 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры _____

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без

		дополнительных занятий по соответствующей дисциплине.
--	--	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания (баллов)
ПК-3: Способен выполнять работы по администрированию процесса управления безопасностью сетевых устройств и программного обеспечения		
Знать:		
- понятия целостность, конфиденциальность, доступность как основных характеристик защищенности информации; - модели политик информационной безопасности в сетях связи; - средства обеспечения защищенного доступа к сетевому оборудованию; - протоколы защищенного информационного обмена в сетях связи; - основные способы организации безопасного соединения через незащищенные общедоступные сети. - принципы функционирования аппаратно-программных средств защиты информации в сетях связи; - принципы внедрения средств защиты информации в сети связи; - принципы мониторинга инцидентов с использованием аппаратно-программных средств защиты информации в сетях связи.	Контрольная работа	Модуль 1 0÷20 «Неудовлетворительно» - 0-5 «Удовлетворительно» - 6-10 «Хорошо» - 11-15 «Отлично» -16-20
		Модуль 2 0÷20 «Неудовлетворительно» - 0-5 «Удовлетворительно» - 6-10 «Хорошо» - 11-15 «Отлично» -16-20
Уметь:		
- классифицировать и оценивать угрозы информационной безопасности в сетях связи; - проводить работы по администрированию средств защиты информации в сетях связи; - использовать механизмы аутентификации и авторизации в сетях связи; - конфигурировать встроенные в сетевое оборудование средства защиты; - проводить работы по разграничению прав доступа пользователей к сетевым ресурсам; - проводить работы по конфигурированию и администрированию аппаратно-программных средств защиты информации в сетях связи.	Практическое занятие 1 Практическое занятие 2 Практическое занятие 3 Практическое занятие 4 Практическое занятие 5	Модуль 1 0÷15 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-8 «Хорошо» - 9-12 «Отлично» - 13-15
		Модуль 2 0÷10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-8 «Хорошо» - 9-12 «Отлично» - 13-15
Владеть:		
- основными понятиями, связанными с обеспечением безопасности в сетях	Лабораторная работа 1 Лабораторная работа 2 Лабораторная работа 3	Модуль 1 0÷15 «Неудовлетворительно» - 0-4

связи; - навыками работы по конфигурированию средств защиты сетей связи; - навыками конфигурирования защищенного удаленного доступа; - навыками конфигурирования средств аутентификации; - навыками конфигурирования аппаратно-программных средств межсетевого экранирования; - навыками конфигурирования аппаратно-программных средств для организации виртуальных частных сетей.	Лабораторная работа 4 Лабораторная работа 5	«Удовлетворительно» - 5-8 «Хорошо» - 9-12 «Отлично» - 13-15
		Модуль 2 0÷10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-8 «Хорошо» - 9-12 «Отлично» - 13-15
	Экзамен	0-100 «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 3 лекционных занятия, 3 практические и 3 лабораторные работы. Знание лекционного материала оценивается по контрольной работе, максимальное количество баллов составляет 20. За каждую выполненную и защищенную лабораторную работу обучающий получает максимум 3 балла общей суммой 15 баллов. При опросе на каждом практическом занятии обучающийся получает максимум 3 балла общей суммой 15 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ПК-3):

1. Определение и классификация политик безопасности.
2. Дискреционная политика безопасности.
3. Мандатная политика безопасности.
4. Ролевая политика безопасности.
5. Методы защиты консольного доступа к сетевому оборудованию.
6. Протоколы удаленного доступа к сетевому оборудованию.
7. Методы защиты удаленного доступа к сетевому оборудованию.
8. Протокол RADIUS.
9. Протокол TACACS+.
10. Логирование сетевых событий.
11. Определение и классификация межсетевых экранов.
12. Межсетевые экраны с пакетной фильтрацией.
13. Межсетевые экраны с сохранением состояний.
14. Межсетевые экраны Zone-Based Policy Firewall (ZBFW).
15. Межсетевые экраны следующего поколения (NGFW).
16. Принцип работы системы обнаружения вторжений (IDS).
17. Принцип работы системы предотвращения вторжений (IPS).

18. Зеркалирование портов для контроля трафика.
19. Требования нормативных документов и технических регламентов к защищенным сетям связи.
20. Технические характеристики аппаратных межсетевых экранов различных производителей.
21. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации.
22. Обеспечение защиты беспроводного сетевого оборудования.
23. Механизмы комплексной защиты сетей электросвязи.
24. Положение о лицензировании деятельности по технической защите конфиденциальной информации.
25. Обеспечение сохранения коммерческой тайны предприятия.
26. Каталог обобщенных мероприятий по защите конфиденциальной информации.
27. Управление обновлениями ПО и ОС.

Практическое занятие №1. Конфигурирование защиты консольного доступа.

Контрольные вопросы (ПК-3):

1. Понятие консольного доступа.
2. Необходимость защиты консольного доступа.
3. Защита перехода в привилегированный режим при консольном доступе.
4. Виды паролей.
5. Создание учетной записи пользователя при консольном доступе.
6. Назначение привилегий учетным записям.
7. Принцип создания списка разрешенных команд.
8. Просмотр учетных записей на устройстве.

Практическое занятие № 2. Конфигурирование защиты удаленного доступа.

Контрольные вопросы (ПК-3):

1. Понятие удаленного доступа.
2. Протоколы удаленного доступа.
3. Защита конфиденциальности информации при удаленном доступе.
4. Процесс установления соединения в протоколе SSHv2.
5. Порядок конфигурирования маршрутизатора как SSH-сервера.
6. Использование учетных записей при удаленном доступе.

Практическое занятие № 3. Конфигурирование защиты удаленного доступа с использованием AAA- и Syslog-серверов.

Контрольные вопросы (ПК-3):

1. Алгоритм аутентификации с использованием AAA-сервера.
2. Протоколы взаимодействия между AAA-сервером и маршрутизатором.
3. Защита конфиденциальности информации при серверной аутентификации.
4. Процесс установления соединения в протоколе TACACS+.
5. Порядок конфигурирования AAA-сервера.
6. Порядок конфигурирования маршрутизатора для взаимодействия с AAA-сервером.

Лабораторная работа №1. Исследование свойств межсетевого экрана с пакетной фильтрацией.

Контрольные вопросы защиты (ПК-3):

1. Назначение межсетевых экранов.
2. Критерии проверки пакетов МСЭ с пакетной фильтрацией.
3. Виды списков управления доступом (ACL).
4. Привязка ACL к интерфейсам маршрутизатора.
5. «Черные» и «белые» ACL.
6. Алгоритм проверки пакетов МСЭ с пакетной фильтрацией.

7. Недостатки МСЭ с пакетной фильтрацией.

Лабораторная работа №2. Исследование свойств межсетевого экрана с сохранением состояний.

Контрольные вопросы защиты (ПК-3):

1. Назначение межсетевых экранов.
2. Критерии инспектирования сессий МСЭ с сохранением состояний.
3. Привязка правил инспектирования к интерфейсам маршрутизатора.
4. Инспектирование протоколов транспортного и прикладного уровней.
6. Алгоритм проверки сессий МСЭ с сохранением состояний.
7. Недостатки МСЭ с сохранением состояний.

Лабораторная работа №3. Исследование свойств межсетевого экрана ZBFW.

Контрольные вопросы защиты (ПК-3):

1. Назначение межсетевых экранов.
2. Понятие зон безопасности.
3. Понятие пар зон безопасности.
4. Этапы конфигурирования межсетевого экрана ZBFW.
6. Понятие Class map.
7. Понятие Policy map.
8. Действия с трафиком, конфигурируемые в Policy map.

Модуль 2: (50 баллов):

Модуль содержит 2 лекционных занятия, 2 практические и 2 лабораторные работы. Знание лекционного материала оценивается по контрольной работе, максимальное количество баллов составляет 20. За каждую выполненную и защищенную лабораторную работу 4 обучающий получает максимум 8 баллов, за лабораторную работу 5 – максимум 7 баллов. Общая суммой баллов за лабораторные работы составляет 15. При опросе на практическом занятии 4 обучающийся получает максимум 8 баллов, на практическом занятии 5 – максимум 7 баллов. Общая суммой баллов за практические занятия составляет 15. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ПК-3):

1. Уровни сетевой защиты.
2. Структура защищенной сети.
3. Методы и средства повышения сетевой доступности.
4. Статический NAT.
5. Динамический NAT.
6. NAT с применением маскардинга.
7. Защита от атак на VLAN.
8. Защита от атак на протокол STP.
9. Использование функции Port Security.
10. Защита от атак на протоколы DHCP и ARP.
11. Определение и классификация VPN.
12. Протоколы VPN, реализуемые на втором уровне модели OSI.
13. Протоколы VPN, реализуемые на третьем уровне модели OSI.
14. Протоколы туннелирования.
15. Протоколы IPSec.
16. Dos и DDos-атаки.

17. Системы обнаружения вторжений (IDS).
18. Системы предотвращения вторжений (IPS).
19. Классификация компьютерных вирусов.
20. Применение антивирусного ПО на шлюзах корпоративной сети.
21. Классификация корпоративного антивирусного ПО.
22. Протоколы PPTP, L2TP, L2PW.
23. Сравнительный анализ протоколов второго уровня.
24. Применение протоколов второго уровня в системе Site-to-Site.
25. Применение протоколов второго уровня в системе Remote VPN.
26. Организационные мероприятия по комплексной защите корпоративной сети.

Практическое занятие №4. Построение локальной сети с комплексной защитой.

Контрольные вопросы (ПК-3):

1. Атаки VLAN Hopping.
2. Защита от атак с использованием протокола DHCP.
3. Защита от атак с использованием протокола ARP.
4. Назначение функции Port Security.
5. Назначение Trunk-портов коммутатора.
6. Защита от атак на протокол STP.
7. Порядок конфигурирования NAT.
8. Просмотр NAT-трансляций на маршрутизаторе.

Практическое занятие №5. Конфигурирование Site-to-Site VPN.

Контрольные вопросы (ПК-3):

1. Назначение VPN.
2. Виды VPN.
3. Протокол AH.
4. Протокол ESP.
5. Понятие Transform Set.
6. Защита от атак на протокол STP.
7. Порядок конфигурирования VPN на маршрутизаторе.
8. Проверка функционирования VPN.
9. Порядок согласования алгоритмов шифрования при установлении защищенного соединения.

Лабораторная работа №4. Исследование повышения доступности сети с виртуальным маршрутизатором.

Контрольные вопросы защиты (ПК-3):

1. Принципы повышения сетевой доступности.
2. Семейство протоколов FHRP.
3. Термины VRRP.
4. VRRP с балансировкой и без балансировки трафика.
6. Использование приоритетов при балансировке трафика.
7. Этапы конфигурирования VRRP.

Лабораторная работа №5. Исследование VPN туннеля.

Контрольные вопросы защиты (ПК-3):

1. Виды VPN туннелей.
2. Виды Remote VPN.
3. Согласование алгоритмов аутентификации, шифрования и проверки целостности.
4. Проверка состояния VPN туннеля.
6. Работа VPN в транспортном и туннельном режимах.

7. Сравнение протоколов АН и ESP.

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Сетевая безопасность» (ПК-3):

1. Определение и классификация политик безопасности.
2. Дискреционная политика безопасности.
3. Мандатная политика безопасности.
4. Ролевая политика безопасности.
5. Методы защиты консольного доступа к сетевому оборудованию.
6. Протоколы удаленного доступа к сетевому оборудованию.
7. Методы защиты удаленного доступа к сетевому оборудованию.
8. Протокол RADIUS.
9. Протокол TACACS+.
10. Логирование сетевых событий.
11. Определение и классификация межсетевых экранов.
12. Межсетевые экраны с пакетной фильтрацией.
13. Межсетевые экраны с сохранением состояний.
14. Межсетевые экраны Zone-Based Policy Firewall (ZBFW).
15. Межсетевые экраны следующего поколения (NGFW).
16. Принцип работы системы обнаружения вторжений (IDS).
17. Принцип работы системы предотвращения вторжений (IPS).
18. Зеркалирование портов для контроля трафика.
19. Требования нормативных документов и технических регламентов к защищенным сетям связи.
20. Технические характеристики аппаратных межсетевых экранов различных производителей.
21. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации.
22. Обеспечение защиты беспроводного сетевого оборудования.
23. Механизмы комплексной защиты сетей электросвязи.
24. Положение о лицензировании деятельности по технической защите конфиденциальной информации.
25. Обеспечение сохранения коммерческой тайны предприятия.
26. Каталог обобщенных мероприятий по защите конфиденциальной информации.
27. Управление обновлениями ПО и ОС.
28. Уровни сетевой защиты.
29. Структура защищенной сети.
30. Методы и средства повышения сетевой доступности.
31. Статический NAT.
32. Динамический NAT.
33. NAT с применением маскардинга.
34. Защита от атак на VLAN.
35. Защита от атак на протокол STP.
36. Использование функции Port Security.
37. Защита от атак на протоколы DHCP и ARP.
38. Определение и классификация VPN.
39. Протоколы VPN, реализуемые на втором уровне модели OSI.
40. Протоколы VPN, реализуемые на третьем уровне модели OSI.
41. Протоколы туннелирования.
42. Протоколы IPSec.
43. Dos и DDos-атаки.

44. Системы обнаружения вторжений (IDS).
45. Системы предотвращения вторжений (IPS).
46. Классификация компьютерных вирусов.
47. Применение антивирусного ПО на шлюзах корпоративной сети.
48. Классификация корпоративного антивирусного ПО.
49. Протоколы PPTP, L2TP, L2PW.
50. Сравнительный анализ протоколов второго уровня.
51. Применение протоколов второго уровня в системе Site-to-Site.
52. Применение протоколов второго уровня в системе Remote VPN.
53. Организационные мероприятия по комплексной защите корпоративной сети.

1.4 Оценочные материалы для заочной и очно-заочной форм обучения

Практическое занятие №1. Конфигурирование защиты консольного и удаленного доступа.

Контрольные вопросы (ПК-3):

1. Понятие консольного доступа.
2. Необходимость защиты консольного доступа.
3. Защита перехода в привилегированный режим при консольном доступе.
4. Виды паролей.
5. Создание учетной записи пользователя при консольном доступе.
6. Назначение привилегий учетным записям.
7. Принцип создания списка разрешенных команд.
8. Просмотр учетных записей на устройстве.
9. Протоколы удаленного доступа.
10. Серверная аутентификация.

Практическое занятие №2. Построение локальной сети с комплексной защитой.

Контрольные вопросы (ПК-3):

1. Атаки VLAN Hopping.
2. Защита от атак с использованием протокола DHCP.
3. Защита от атак с использованием протокола ARP.
4. Назначение функции Port Security.
5. Назначение Trunk-портов коммутатора.
6. Защита от атак на протокол STP.
7. Порядок конфигурирования NAT.
8. Просмотр NAT-трансляций на маршрутизаторе.

Лабораторная работа №1. Исследование свойств межсетевых экранов.

Контрольные вопросы защиты (ПК-3):

1. Назначение межсетевых экранов.
2. Критерии проверки пакетов МСЭ с пакетной фильтрацией.
2. Критерии инспектирования сессий МСЭ с сохранением состояний.
3. Привязка правил инспектирования к интерфейсам маршрутизатора.
4. Привязка ACL к интерфейсам маршрутизатора.
6. Алгоритм проверки сессий МСЭ с сохранением состояний.
7. Порядок конфигурирования МСЭ ZBFW.

Лабораторная работа №2. Исследование повышения доступности сети с виртуальным маршрутизатором.

Контрольные вопросы защиты (ПК-3):

1. Принципы повышения сетевой доступности.
2. Семейство протоколов FHRP.
3. Термины VRRP.
4. VRRP с балансировкой и без балансировки трафика.
6. Использование приоритетов при балансировке трафика.
7. Этапы конфигурирования VRRP.

Вопросы, выносимые на экзамен по дисциплине «Сетевая безопасность» (ПК-3):

1. Определение и классификация политик безопасности.
2. Дискреционная политика безопасности.
3. Мандатная политика безопасности.
4. Ролевая политика безопасности.
5. Методы защиты консольного доступа к сетевому оборудованию.
6. Протоколы удаленного доступа к сетевому оборудованию.
7. Методы защиты удаленного доступа к сетевому оборудованию.
8. Протокол RADIUS.
9. Протокол TACACS+.
10. Логирование сетевых событий.
11. Определение и классификация межсетевых экранов.
12. Межсетевые экраны с пакетной фильтрацией.
13. Межсетевые экраны с сохранением состояний.
14. Межсетевые экраны Zone-Based Policy Firewall (ZBFW).
15. Межсетевые экраны следующего поколения (NGFW).
16. Принцип работы системы обнаружения вторжений (IDS).
17. Принцип работы системы предотвращения вторжений (IPS).
18. Зеркалирование портов для контроля трафика.
19. Требования нормативных документов и технических регламентов к защищенным сетям связи.
20. Технические характеристики аппаратных межсетевых экранов различных производителей.
21. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации.
22. Обеспечение защиты беспроводного сетевого оборудования.
23. Механизмы комплексной защиты сетей электросвязи.
24. Положение о лицензировании деятельности по технической защите конфиденциальной информации.
25. Обеспечение сохранения коммерческой тайны предприятия.
26. Каталог обобщенных мероприятий по защите конфиденциальной информации.
27. Управление обновлениями ПО и ОС.
28. Уровни сетевой защиты.
29. Структура защищенной сети.
30. Методы и средства повышения сетевой доступности.
31. Статический NAT.
32. Динамический NAT.
33. NAT с применением маскардинга.
34. Защита от атак на VLAN.
35. Защита от атак на протокол STP.
36. Использование функции Port Security.
37. Защита от атак на протоколы DHCP и ARP.
38. Определение и классификация VPN.

39. Протоколы VPN, реализуемые на втором уровне модели OSI.
40. Протоколы VPN, реализуемые на третьем уровне модели OSI.
41. Протоколы туннелирования.
42. Протоколы IPSec.
43. Dos и DDos-атаки.
44. Системы обнаружения вторжений (IDS).
45. Системы предотвращения вторжений (IPS).
46. Классификация компьютерных вирусов.
47. Применение антивирусного ПО на шлюзах корпоративной сети.
48. Классификация корпоративного антивирусного ПО.
49. Протоколы PPTP, L2TP, L2PW.
50. Сравнительный анализ протоколов второго уровня.
51. Применение протоколов второго уровня в системе Site-to-Site.
52. Применение протоколов второго уровня в системе Remote VPN.
53. Организационные мероприятия по комплексной защите корпоративной сети.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

2.1 Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- промежуточный контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- промежуточный контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты лабораторных и практических занятий проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы (практического занятия) – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний студентов теоретической части лабораторной работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки студентом практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения студентов к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности студентов в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0% до 40% от максимального количества баллов;
- «удовлетворительно» - от 41% до 60% максимального количества баллов;

- «хорошо» - от 61% до 80% максимального количества баллов;
- «отлично» - от 81% до 100% максимального количества баллов.

Соотношения максимального количества баллов, полученных студентом по блокам модулей, показаны в Таблице 2.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице

Таблица - Распределение баллов по блокам модулей дисциплины «Сетевая безопасность»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	20	30
Модуль 2	50	20	30
Модуль - Экзамен	100		

Результаты текущего контроля доводятся до сведения обучающихся на последнем занятии до проведения промежуточной аттестации.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

2.2 Методика проведения экзамена в группах заочной и очно-заочной форм обучения

Экзамен по дисциплине «Сетевая безопасность» у обучающихся заочной и очно-заочной форм обучения проводится письменно по классической методике. Вопросы сгруппированы в билетах. В каждом билете содержится по 2 вопроса, скомпонованные таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины. Количество билетов должно быть не менее числа обучающихся в группе. Обучающиеся готовят письменные ответы на вопросы.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в устном виде. Количество вопросов в экзаменационном билете – 2. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку обучающегося.

Обучающиеся, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Образец экзаменационного билета

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИТСС» _____ « ____ » _____ 20__ г.
	Направление подготовки: 09.03.02 Инфокоммуникационные технологии и системы связи Курсы: 4 Дисциплина: Сетевая безопасность	
Билет №7 1. Межсетевые экраны с пакетной фильтрацией. 2. Протокол RADIUS. Доцент каф. «ИТСС» _____ Манин А.А. « ____ » _____ 20__ г.		

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания для проведения оценки сформированности компетенции ПК-3

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ПК-2 равно 20, по компетенции ПК-3 равно 20. Всего 40 заданий

Ключи к ответам представлены в отдельных таблицах.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ за дания	Тексты заданий
1	Дискреционная политика безопасности предполагает ____ 1. определение прав доступа субъектов к объектам 2. соотношение атрибутов безопасности объектов уровню доступа субъекта 3. определения множеств пользователей, ролей, полномочий и сеансов
2	Мандатная политика безопасности предполагает ____

№ за дания	Тексты заданий
	1. определение прав доступа субъектов к объектам 2. соотношение атрибутов безопасности объектов уровню доступа субъекта 3. определения множеств пользователей, ролей, полномочий и сеансов
3	Ролевая политика безопасности предполагает ____ 1. определение прав доступа субъектов к объектам 2. соотношение атрибутов безопасности объектов уровню доступа субъекта 3. определения множеств пользователей, ролей, полномочий и сеансов
4	Пароль enable password хранится ____ 1. на устройстве в зашифрованном виде 2. на AAA-сервере 3. на устройстве в незашифрованном виде
5	Пароль enable secret хранится ____ 1. на устройстве в зашифрованном виде 2. на AAA-сервере 3. на устройстве в незашифрованном виде
6	Удаленный доступ к устройствам производится с использованием ____ интерфейсов 1. виртуальных 2. физических 3. сетевых
7	Протокол Telnet обеспечивает передачу данных 1. в незашифрованном виде 2. в зашифрованном виде 3. в кодированном виде
8	Протокол SSH обеспечивает передачу данных 1. в незашифрованном виде 2. в зашифрованном виде 3. в кодированном виде
9	AAA-сервер предназначен 1. для хранения файлов и данных 2. для централизованного управления доступом 3. для обеспечения функционирования службы DNS
10	При использовании AAA-сервера локальная учетная запись применяется для - исключения физического доступа к оборудованию 1. обеспечения доступа к устройству в случае отказа AAA-сервера 2. обеспечения доступа к AAA-серверу 3. Обеспечения доступа к Интернет

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Расставьте команды конфигурирования в соответствии с их действием 1. aaa new-model 2. port security 3. vlan № 4. username <логин> 5. login local

№ задания	Тексты заданий
	А. Включает функцию защиты портов коммутаторов от НСД Б. Создает учетную запись пользователя В. Включает на сетевом устройстве функцию AAA Г. Создает на коммутаторе виртуальную локальную сеть Д. Указывает на необходимость аутентификации по локальной базе
12	Установите соответствие сетевых средств защиты их назначению: 1. Зональный межсетевой экран; 2. Межсетевой экран с сохранением состояний; 3. IDS/IPS; 4. NAC; А. Средства контроля доступа в сеть; Б. Разделение сети на защищенные сегменты, в том числе DMZ; В. Защита периметра сети; Г. Средства обнаружения/предотвращения вторжений.
13	Существуют следующие уровни сетевой защиты: 1. Internet Layer; 2. Perimeter Layer; 3. Network Layer; 4. Endpoint Layer; 5. User Layer. Поставьте в соответствие определения данных уровней: А. поиск и предотвращение угроз вне периметра защищаемой сети. Б. предназначен для анализа внутрисетевого трафика на предмет компрометации локальных узлов. В. предназначен для максимального сокращения площади атаки на сеть. Г. повышение защищенности сети через обучение корпоративных пользователей основам информационной безопасности. Д. предназначен для комплексной защиты рабочих станций и мобильных устройств.
14	Для безопасности сетевых устройств характерны следующие риски: 1. Подключение неучтенного оконечного оборудования; 2. Консольное подключение с правами администратора; 3. Удаленное подключение с правами администратора. Для защиты от этих рисков используется: А. Серверная аутентификация; Б. Аутентификация по локальной базе; В. Технология Port Security.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в порядке увеличения количества доступных команд конфигурирования привилегии: 1. Пользовательский режим 2. Привилегированный режим 3. Режим глобального конфигурирования
16	Расставьте по порядку этапы установления соединения VPN IPSec: 1. Передача данных

№ задания	Тексты заданий
	2. Установление защищенного ISAKMP-канала 3. Установление защищенного IPSec-канала 4. Взаимная аутентификация
17	Расставьте в порядке значимости нормативные акты, регламентирующие вопросы информационной безопасности: 1. Локальные нормативные акты; 2. Приказы соответствующих Министерств и Ведомств; 3. Законы РФ; 4. Указы Президента РФ; 5. Конституция РФ; 6. Постановления Правительства РФ.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Для чего предназначена технология Site-to-Site VPN? _____
19	Что является объектом в модели политики информационной безопасности? _____
20	Что такое атаки VLAN Hopping? _____

Методика проведения тестирования

Максимальное время выполнения теста - 60 минут.

Количество тестовых заданий в тесте не менее 20.

Для проведения контроля остаточных знаний компьютер формирует в случайном порядке 60 тестовых заданий.

При прохождении тестового контроля знаний обучающийся должен выбрать один или несколько правильных ответов в каждом тестовом задании.

В случае правильного ответа на 17 и более тестовых заданий (81-100% правильных ответов) обучающийся подтверждает освоение компетенций с уровнем «отлично». При ответе на 13-16 тестовых заданий (61-80% правильных ответов) обучающийся подтверждает освоение компетенций с уровнем «хорошо». При ответе на 9-12 тестовых заданий (41-60% правильных ответов) обучающийся подтверждает освоение компетенций с уровнем «удовлетворительно». При ответе менее чем на 9 тестовых заданий (0-40% правильных ответов) обучающийся не подтверждает необходимый уровень знаний и оценивается «неудовлетворительно».

Критерии оценивания ответов на тестовые задания ПК-3

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания С 1-по 10	Блок А Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы. 50% тестовых заданий.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания С 11-по 17	Блок Б Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого). 20% тестовых заданий	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
	Блок Б Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр. 15% тестовых заданий	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует - 0 баллов.
	Блок В Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте. 15% тестовых заданий	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Дисциплина «Сетевая безопасность» включает в себя:

- лекционные занятия – 10 часов;
- практические занятия – 20 часов;
- лабораторные работы – 20 часов;
- промежуточную аттестацию – экзамен.

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемых в работе задач.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и контроля знаний обучающихся при проведении промежуточной аттестации.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по подготовке к лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать

изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующем данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.