

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

«28» _____ 2026 г.

Рабочая программа дисциплины

Б1.О.36.06

**Администрирование средств защиты информации в компьютерных
системах и сетях**

Кафедра: **Информационная безопасность**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в
сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФ	
	ЗЕ	Часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/8
Контактная работа, в том числе (по семестрам, курсам):		70/8
Лекции		18/8
Лабораторных работ		18/8
Практических занятий		34/8
Семинаров		
Самостоятельная работа		38/8
Контроль		36/8
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/8

Программу составил:
Кандидат технических наук, с.н.с. Ткачук Е.О.

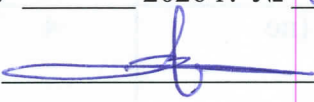
Рабочая программа дисциплины
«Администрирование средств защиты информации в компьютерных системах и сетях»

Разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026 г., и утвержденного директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационной безопасности

Протокол от «28» 04 2026 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины «Администрирование средств защиты информации в компьютерных системах и сетях» является теоретическая и практическая подготовка, которая должна обеспечить получение у обучающихся углубленных представлений о современных методах защиты информации в сложных компьютерных системах и сетях, способах их реализации и применения.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с **эксплуатационным** видом деятельности:

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях	
Знать:	
- принципы построения компьютерных сетей - стек сетевых протоколов операционных систем - стек протоколов сетевого оборудования - порядок реализации методов и средств межсетевого экранирования - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	
Уметь:	
- производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях - использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации;	
Владеть:	
- мерами по нейтрализации источников угроз; - навыками построения типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; - методами измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; - навыками работы и правилами эксплуатации программно-аппаратных средств защиты информации.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Администрирование средств защиты информации в компьютерных системах и сетях» является логическим продолжением дисциплины Б1.О.25 «Основы информационной безопасности», знание которой в объеме требований образовательной программы является необходимым
2	Успешное освоение дисциплины «Администрирование средств защиты информации в компьютерных системах и сетях» базируется также на знаниях, приобретенных из дисциплин: Б1.О.06 «Высшая математика», Б1.О.07 «Иностранный язык», Б1.О.12 «Информационная экология».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	

1	Дисциплина является базовой для успешного освоения дисциплин: Б2.В.03(Пд) Производственная (преддипломная) практика; Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы
---	---

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 72 аудиторных часов, 72 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компет енции	УМИО
Курс 4, Семестр 8					
Модуль 1. Общие принципы администрирования информационных систем. (36+24) часов					
1.1	Лекция 1. АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ. Вводные положения. Функции администратора системы. Состав служб администратора системы и их назначение. Требования к специалистам. Стандарты работы ИС и стандартизирующие организации. Объекты администрирования и модели управления. Модель сетевого управления ISO. Модель FCAPS. Модель ITIL. Модель TMN. Модель e ГОМ. Модель RPC	Лек 1	2	ОПК-1.2	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. АДМИНИСТРИРОВАНИЕ КАБЕЛЬНЫХ СИСТЕМ И СЕТЕВЫХ СИСТЕМ Администрирование кабельных систем. Понятие о средах передачи. Кабельные системы передачи данных. Стандарты и задачи администрирования кабельных систем. Управление коммутаторами. Вопросы проектирования сети. Понятие систем сетевого администрирования.	Лек 2	2	ОПК-1.2	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. СРЕДСТВА АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ. АДМИНИСТРИРОВАНИЕ ФАЙЛОВЫХ СИСТЕМ. Средства администрирования операционных систем. Администрирование файловых систем. Параметры ядра ОС. Установка ОС. Подсистема ввода/вывода и способы организации дискового пространства. Технология RAID. Файловые системы Интернет.	Лек 3	2	ОПК-1.2	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие 1. Администрирование адресации компьютеров в локальной сети. MAC адрес, IP адрес, понятие URL. Маска подсети. Выдача задания на курсовую работу.	ПЗ1	8	ОПК-1.2	Л3.1
1.5	Практическое занятие 2. Программное обеспечение администрирования сетей ЭВМ Программное обеспечение вычислительных сетей; Возможности сетевых операционных сред. Анализ корректности архитектуры сети Ethernet в соответствии с индивидуальным вариантом.	ПЗ2	8	ОПК-1.2	Л3.1

1.6	Лабораторная работа 1. Способы подключения оптоволоконных мультиплексоров Изучение способов подключения оптоволоконных мультиплексоров и проверки соединения оптоволоконных систем.	ЛР1	6	ОПК-1.2	ЛЗ.1
1.7	Лабораторная работа № 2. Способы соединения сетевых устройств. Способы соединения сетевых устройств. Подключение рабочих станций к коммутатору и установка параметров ОС. Проверка соединения	ЛР2	6	ОПК-1.2	ЛЗ.1
1.8	1.Оптоволоконные кабельные системы. Изучение методов терминирования и сплайсирования оптоволоконных кабельных систем. 2.Создание элементов структурированной кабельной системы. Горизонтальная подсистема. Подсистема рабочего места. 3.Изучение топологии сетевых систем. Способы соединения, диагностики и тестирования кабельной системы на основе витой пары. 4. Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	СРС	19	ОПК-1.2	Л1.1 Л1.2 Л1.3

Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях (36+24)

2.1	Лекция 4. АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ. Администрирование баз данных. Средства СУБД. Администрирование данных. Инсталляция СУБД. Параметры ядра СУБД и параметры ввода/вывода. Средство мониторинга и сбора статистики. Средства защиты от несанкционированного доступа. Способы восстановления и реорганизации БД. Стратегии администратора БД.	Лек 4	4	ОПК-1.2	Л1.1 Л1.2 Л1.3
2.2	Лекция 5. АДМИНИСТРИРОВАНИЕ ПРОЦЕССА ПОИСКА И ДИАГНОСТИКИ ОШИБОК. Администрирование процесса поиска и диагностики ошибок. 12 задач управления при обнаружении ошибки ИС. Базовая модель поиска ошибки. Стратегия определения ошибок. Средства сбора и поиска ошибок администратора системы. Метрика работы ИС. Примеры диагностики ошибок для технологии Ethernet и для среды протоколов ТСП/ІР. Предупреждение ошибок и решение проблем в среде протоколов ТСП/ІР.	Лек 5	4	ОПК-1.2	Л1.1 Л1.2 Л1.3
2.3	Лекция 6. АДМИНИСТРИРОВАНИЕ ПРОЦЕССА КОНФИГУРАЦИИ, ПРОЦЕССА УЧЕТА И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Администрирование процесса конфигурации. Задачи и проблемы конфигурации. Оценки эффективности конфигурации с точки зрения бизнеса.	Лек 6	4	ОПК-1.2	Л1.1 Л1.2 Л1.3

	Администрирование процесса учета и обеспечения информационной безопасности. Задачи учета. Защита от угроз безопасности. Средства, мероприятия и нормы обеспечения безопасности. Пример реализации защиты от НСД для ИС. Пример реализации средств безопасности для сетевой подсистемы ИС.				
2.4	Практическое занятие 3 Канальный уровень модели OSI: Протокол LLC. Реализация LLC. Протоколы канального уровня.	ПЗ 3	6	ОПК-1.2	ЛЗ.1
2.5	Практическое занятие 4. Диагностика Ethernet и TCP/IP Средства диагностики Ethernet и TCP/IP. Утилита PING. Диагностика Ethernet и TCP/IP. Утилита Traceroute. Изучение средств отладки соединений	ПЗ 4	6	ОПК-1.2	ЛЗ.1
2.6	Практическое занятие 5 Администрирование адресации устройств Изучение вопросов адресации устройств. Конфигурация протокола ARP	ПЗ5	6	ОПК-1.2	ЛЗ.1
2.7	Лабораторная работа № 3 Администрирование коммутации пакетов в сетях Способы управления коммутатором. Задание базовых параметров ОС коммутатора. Изучение методов защиты от несанкционированного доступа.	ЛР3	6	ОПК-1.2	ЛЗ.1
2.8	1.Способы реализации протоколов IEEE 802.1xx. Настройка VLAN коммутатора. 2.Изучение управления портом коммутатора 100-Base Ethernet. Задание параметров порта. Проверка состояния. 3.Изучение вопросов адресации устройств. Конфигурация протокола ARP. 4.Изучение протоколов маршрутизации. Конфигурация протокола RIP.	СРС	19	ОПК-1.2	Л1.1 Л1.2 Л1.3
	Экзамен		36	ОПК-1.2	Л1.1 Л1.2 Л1.3
Итого – 144 часов					

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	Гаспариан, М. С. Н. Лихачева.	Информационные системы и технологии : учебное пособие.	Москва : Евразийский открытый институт, 2011. — 370 с.	Э1
Л1.2	Семакин И.Г. Хеннер Е.К.-	Информационные системы и модели	М.: БИНОМ. Лаборатория знаний, 2012.- 71 с.	Э2
Л1.3	Фомин, Д. В.	Информационная безопасность: учебник	Москва : Ай Пи Ар Медиа, 2022. — 222 с.	Э3
5.1.2. Дополнительная литература				

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Гатчин Ю.А., Климова Е.В.	Введение в комплексную защиту объектов информатизации	СПб.: Университет ИТМО, 2011. — 112 с.	Э4
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Нестеров С.А.	Основы информационной безопасности [Электронный ресурс]: учебное пособие/— Электрон. текстовые данные.	СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с.	Э5
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/10680.html			
Э2	http://www.ip1-bookshop.ru/6473			
Э3	https://www.iprbookshop.ru/118876.html			
Э4	http://www.iprbookshop.ru/65808.html			
Э5	https://www.iprbookshop.ru/43960			
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/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
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/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.7	Электронный ресурс http://www.securitylab.ru/			
5.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	1. AVAST Free Antivirus		Антивирусное ПО. Свободное, условно свободное или триал-версии.	
	2. AVG AntiVirus Free			
	3. Dr.Web Antivirus			
	4. Антивирус Касперского			
	5. ESET NOD32 Антивирус			
	6. AVZ Antivirus			
	7. Avira Free Antivirus			
	8. Norton AntiVirus			
	9. McAfee Antivirus			

	10. Emsisoft Anti-Malware 11. BullGuard Antivirus 12. Protector Plus Antivirus 13. Panda Antivirus 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus	
II.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
II.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
II.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Paragon Rescue Kit 7. Wise Data Recovery 8. Puran File Recovery 9. O&O DiskRecovery 10. Tenorshare Any Data Recovery 11. Power Data Recovery 12. GetDataBack 13. Recover My Files 14. R-Undelete 15. Handy Recovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

	16. Ashampoo Undeleter	
П.5	1. Iperius Backup 2. FBackup 3. Backup4all 4. Uranium Backup Free 5. Simple Data Backup 6. Personal Backup 7. Back4Sure 8. SyncBackFree 9. Handy Backup 10. EASEUS Todo Backup 8.0 Free Edition 11. Exiland Backup Free 4.0 12. Nero BackItUp 13. Paragon Rescue Kit 14.0 Free 14. Action Backup 15. LimBackup 16. AVSbackup 17. ExtraBackup 18. Cobian Backup 19. Backup & Recovery 10 Build 9169 Free Edition 20. Information Backup System	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

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	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации
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 для обучающихся 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, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Администрирование средств защиты информации в компьютерных системах и сетях Б1.О.36.06» для использования в 20__/20__ учебном году

Утверждаю

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

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(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 ИБ

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, дает полные, профессиональные и грамотные ответы на поставленные вопросы, что свидетельствует об освоении обучающимся взаимосвязи основных понятий дисциплины; усвоил основную и знаком с дополнительной рекомендованной литературой; проявляет творческие способности в понимании, изложении и использовании учебно-программного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знания основного и дополнительного учебного материала, дает в целом грамотные ответы на поставленные вопросы, что свидетельствует об освоении обучающимся взаимосвязи основных понятий дисциплины; усвоил основную и знаком с дополнительной рекомендованной литературой. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся демонстрирует знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; в целом отвечает на поставленные вопросы, допуская не принципиальные ошибки; знаком с основной литературой. Допускает ошибки в ответах различного уровня, которые исправляет после наводящих вопросов и под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает существенные пробелы в знаниях основного учебно-программного материала, допустившему 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
ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях		
Знать:		
- принципы построения компьютерных сетей - стек сетевых протоколов операционных систем - стек протоколов сетевого оборудования - порядок реализации методов и средств межсетевого экранирования - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	Тестовый контроль	Модуль 2 0÷10 «Неудовлетворительно» - 0-2 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
Уметь		
- производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях - использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации;	Практические занятия 1-5	Модуль 2 0÷10 за каждое ПЗ «Неудовлетворительно» - 0-2 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
Владеть		
- мерами по нейтрализации источников угроз; - навыками построения типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; - методами измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; - навыками работы и правилами эксплуатации эксплуатируемых программно-аппаратных средств защиты информации.	Лабораторная работа 1-3	Модуль 2 0÷10 за каждое ЛР «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
Экзамен		0-100 баллов «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 средства текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 3 лекционных занятия, 2 лабораторных работы и 2 практических занятия. Знание лекционного материала оценивается по результатам тестового контроля, как выполнения письменных заданий или устных опросов, максимальное количество баллов - 10. За выполненные и защищенные лабораторные работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы тестовых заданий для контроля лекционного материала (ОПК-1.2):

1. Стандарты работы ИС и стандартизирующие организации. Объекты администрирования и модели управления.
2. Модель сетевого управления ISO. Модель FCAPS. Модель ITIL. Модель TMN. Модель e ГОМ. Модель RPC
3. Администрирование кабельных систем. Понятие о средах передачи. Кабельные системы передачи данных.
4. Стандарты и задачи администрирования кабельных систем.
5. Управление коммутаторами. Вопросы проектирования сети.
6. Понятие систем сетевого администрирования
7. Средства администрирования операционных систем.
8. Администрирование файловых систем.
9. Подсистема ввода/вывода и способы организации дискового пространства.
10. Технология RAID.
11. Файловые системы Интернет.

Практическое занятие 1. Администрирование адресации компьютеров в локальной сети

Контрольные вопросы ПЗ №1 ОПК-1.2

1. Мас адрес и его структура.
2. ip- адрес и его структура.
3. Для чего применяется маска подсети.
4. Какие есть специальные ip – адреса.
5. Что произойдет, если в таблицу arp добавить две или более записей, в которых одному мас-адресу сопоставлены разные сетевые адреса?
6. Что произойдет, если в таблицу arp добавить две или более записей, в которых одному сетевому адресу сопоставлены разные аппаратные адреса?
7. Как отличается "время жизни" динамических и статических записей в таблице arp?
8. Почему в ip-сетях не используется прямое сопоставление символьного адреса физическому адресу?
9. Что произойдет, если в файл hosts записать два (или более) узла с одинаковыми именами (например, myhost.mydomain), но разными сетевыми адресами, а затем обратиться к ним по имени (например так: ping myhost.mydomain)

Практическое занятие 2. Программное обеспечение администрирования сетей ЭВМ

Контрольные вопросы ПЗ №2 (ОПК-1.2):

1. Дайте определение понятию «коммуникационная сеть» (ОПК-1.2).
2. Дайте определение понятию «информационная сеть» (ОПК-1.2).
3. Дайте определение понятию «вычислительная (компьютерная) сеть» (ОПК-1.2).
4. Дайте определение понятию «локальная вычислительная сеть (ЛВС)» (ОПК-1.2).

5. Дайте определение понятию «корпоративная вычислительная сеть» (ОПК-1.2).
6. Дайте определение понятию «глобальная вычислительная сеть» (ОПК-1.2).
7. Дайте определение понятию «рабочая группа» (ОПК-1.2).
8. Дайте определение понятию «домен (domain)» (ОПК-1.2).
9. Дайте определение понятию «узел (host)» (ОПК-1.2).
10. Дайте определение понятию «топология (topology)» (ОПК-1.2).
11. Дайте определение понятию «сетевая архитектура» (ОПК-1.2).
12. Дайте определение понятию «программное обеспечение компьютерных сетей»

Лабораторная работа 1. Способы подключения оптоволоконных мультиплексоров

Контрольные вопросы ЛР№1 (ОПК-1.2):

1. Протокол TCP/IP.
2. IP-адреса.
3. Статический IP-адрес.
4. Автоматическое получение IP-адреса.
5. Управляющие протоколы Интернета.
6. Тестирование TCP/IP.
7. Маршрутизация пакетов в IP сетях.
8. Утилиты командной строки для работы с сетью.
9. Служба имен доменов.
10. Пространство имен домена.
11. Разрешение имени.
12. Прямой и обратный запросы.

Лабораторная работа 2. Способы соединения сетевых устройств.

Контрольные вопросы ЛР№2 (ОПК-1.2):

1. Перечислите основные функции протокола ARP в ЛВС?
2. Укажите методы получения информации о неизвестных физических адресах?
3. Перечислите типы записей, используемые в таблице кеша ARP?
4. Воспользовавшись планом сети, укажите значения полей в заголовке кадра Ethernet (IP-адрес отправителя, MAC-адрес отправителя, IP-адрес получателя, MAC-адрес получателя) при передаче кадра от узла PC1 к узлу PC2 и от узла PC1 к узлу PC4?
5. Дайте краткое описание принципов функционирования и отличительные особенности протоколов ARP, RARP, inARP?
6. Изобразите заголовок ARP и укажите назначение основных полей заголовка?
7. Заполните заголовок ARP для следующих сценариев работы компьютерной сети передачи данных:
 - Хост А (MAC C0:F8:DA:11:23:43, IP 10.10.0.2) отправляет широковещательный ARP-запрос, для поиска аппаратного адреса удаленного узла В (MAC C0:F8:DA:11:22:58, IP 10.10.0.5);
 - Хост В отправляет ARP-ответ узлу А.
8. Добавьте к изображенному ранее заголовку ARP, заголовок Ethernet-II DIX, для обоих перечисленных случаев.

Модуль 2: (50 баллов):

Модуль содержит 3 лекционных занятия и 2 практических занятия и 1 лабораторную работу. Знание лекционного материала оценивается по результатам тестового контроля, как выполнения письменных заданий или устных опросов, максимальное количество баллов - 10. За выполненные и защищенные лабораторных работы и практические занятия

обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы тестовых заданий для контроля лекционного материала (ОПК-1.2):

1. Администрирование баз данных. Средства СУБД. Администрирование данных.
2. Установка СУБД. Параметры ядра СУБД и параметры ввода/вывода.
3. Средство мониторинга и сбора статистики.
4. Средства защиты от несанкционированного доступа.
5. Способы восстановления и реорганизации БД.
6. Стратегии администратора БД
7. Администрирование процесса поиска и диагностики ошибок.
8. 12 задач управления при обнаружении ошибки ИС.
9. Базовая модель поиска ошибки. Стратегия определения ошибок.
10. Средства сбора и поиска ошибок администратора системы.
11. Метрика работы ИС. Примеры диагностики ошибок для технологии Ethernet и для среды протоколов TCP/IP.
12. Предупреждение ошибок и решение проблем в среде протоколов TCP/IP.
13. Администрирование процесса конфигурации. Задачи и проблемы конфигурации.
14. Оценки эффективности конфигурации с точки зрения бизнеса.
15. Администрирование процесса учета и обеспечения информационной безопасности.
16. Задачи учета. Защита от угроз безопасности.
17. Средства, мероприятия и нормы обеспечения безопасности.
18. Пример реализации защиты от НСД для ИС.
19. Пример реализации средств безопасности для сетевой подсистемы ИС.

Практическое занятие 3 Канальный уровень модели OSI

Контрольные вопросы ПЗ №3 (ОПК-1.2):

1. В чем заключается основной принцип работы устройств: концентратор, хаб, повторитель?
2. Укажите недостатки структурирования сети на основе концентраторов?
3. Используя схему сети, приведите пример передачи кадров от узла отправителя к узлу получателю?
4. Каким из указанных в проекте устройств необходимо наличие физических адресов (MAC)?
5. Какую логическую топологию выстраивает сетевой концентратор? Какую физическую топологию сети используют при применении концентраторов?
6. В каком режиме разделения общей среды передачи данных функционирует концентратор?
7. Опишите сценарий возникновения и обработки коллизии в сети передачи данных, основанной на применении концентраторов?
8. Перечислите наиболее распространенные типы физических сетевых разъемов и номенклатуру соединительных кабелей, используемых на концентраторах?
9. Укажите назначение Uplink-порта на Ethernet-концентраторе и назначение тумблера Normal/Uplink?

Практическое занятие 4. Диагностика Ethernet и TCP/IP

Контрольные вопросы ПЗ №2 (ОПК-1.2):

1. Перечислите набор стандартов IEEE для организации беспроводной связи WiFi?
2. Укажите рабочие частотные диапазоны стандартов 802.11a, 802.11b, 802.11g и 802.11n?

3. Объясните назначение и функции следующего оборудования: беспроводная сетевая
4. карта (WIC), точка доступа (AP), беспроводной маршрутизатор (WR)?
5. В чем заключается различие между топологиями беспроводной сети Ad-hoc и Hotspot?
6. Укажите способы аутентификации беспроводного клиента? Приведите примеры практического использования указанных способов?
7. Приведите способы защиты доступа к информационной структуре беспроводной сети?
8. Дайте определение понятиям: SSID, WPA, WEP, WLAN, OFDM, DSSS?
9. Укажите методы первоначального конфигурирования класса беспроводного оборудования?
10. Объясните необходимость назначения IP-адреса беспроводной точке доступа?

Лабораторная работа № 3 Администрирование коммутации пакетов в сетях

Контрольные вопросы ЛР№3 (ОПК-1.2):

1. Укажите отличительные особенности в принципах работы концентратора и коммутатора? Приведите пример, основываясь на схеме проекта.
2. Каким из указанных в проекте устройств необходимо наличие физических адресов (MAC)?
3. Перечислите режимы коммутации?
4. Приведите разновидности коммутаторов?
5. Объясните, в чем заключается преимущество агрегирования коммутаторов?
6. Что представляет собой логическое объединение коммутаторов в стек?
7. Укажите методы физического подключения для управления современными коммутаторами? Перечислите основные сетевые протоколы управления активным оборудованием компьютерных сетей передачи данных?
8. Выделите отличительные особенности асимметричной и симметричной коммутации?
9. Вычислите пропускную способность внутренней шины коммутации, если коммутатор работает в неблокирующем режиме и имеет 8 FastEthernet-портов?

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Администрирование средств защиты информации в компьютерных системах и сетях» (ОПК-1.2) (промежуточная аттестация)

1. В рамках какого веб-сервера работают приложения ASP.NET?
2. В чем заключаются функции администратора базы данных?
3. Дайте классификацию и опишите назначение сетевых языков.
4. Дайте классификацию сетевых моделей.
5. Дайте классификацию топологий компьютерных сетей.
6. Дайте понятие локальной, корпоративной и глобальной сетей.
7. Дайте характеристику канальному уровню модели OSI.
8. Дайте характеристику прикладного уровня модели OSI.
9. Дайте характеристику сеансового уровня модели OSI.
10. Дайте характеристику сетевому уровню модели OSI.
11. Дайте характеристику транспортному уровню модели OSI.
12. Дайте характеристику уровню представления данных модели OSI.
13. Для чего используется протокол ICMP? Протокол ARP?
14. Для чего необходимы технологии разработки веб-приложений (такие как ASP.NET, PHP, Ruby On Rails и др.).
15. Как работает защищенный протокол HTTPS?
16. Как работает протокол HTTP и для чего он нужен?
17. Каким образом в HTTP-сообщении заголовки отделяются от тела сообщения?
18. На основе каких интерфейсов может взаимодействовать веб-сервер и веб-приложение?

19. Назовите наиболее популярные реализации веб-серверов.
20. Назовите функции канального, сетевого и транспортного уровней модели OSI.
21. Опишите классы IP-адресов.
22. Опишите методы защиты сетей и применение межсетевых экранов.
23. Опишите назначение и принцип действия протокола TELNET.
24. Опишите назначение и принцип работы протокола ARP.
25. Опишите назначение и принцип работы протокола FTP.
26. Опишите назначение и принцип работы протокола POP3.
27. Опишите назначение и принцип работы протокола PPP.
28. Опишите назначение и принцип работы протокола SLIP.
29. Опишите назначение и принцип работы протокола UDP.
30. Опишите назначение и принцип работы технологии FDDI.
31. Опишите назначение и принципы работы электронной почты.
32. Опишите назначение и работу протокола TCP.
33. Опишите назначение, принцип работы и разновидности брандмауэров.
34. Опишите принцип работы и назначение протокола SMTP.
35. Опишите принцип работы концентраторов и сетевых мостов).
36. Опишите принцип работы сетевой технологии ETHERNET.
37. Опишите принцип работы сетевых устройств (коммутаторов и маршрутизаторов).
38. Опишите принципы адресации хостов сети.
39. Опишите протокол IP, его основные задачи.
40. Опишите работу сетевых мостов.
41. Опишите работу сетевых шлюзов.
42. Опишите способ передачи данных в сетях с коммутацией пакетов.
43. Опишите способы передачи данных в сетях с коммутацией каналов.
44. Опишите структуру и принципы адресации хостов в INTERNET.
45. Опишите цикл обработки запроса к веб-приложению от клиента.
46. Охарактеризуйте каждый из уровней архитектуры ANSI-SPARC. Опишите назначение и принцип работы протокола ICMP.
47. Перечислите и дайте краткое описание служб INTERNET.
48. Поддержка в J2EE
49. Поясните принцип работы утилиты ping.
50. Поясните принцип работы утилиты tracer
51. Поясните, для чего предназначена модель OSI? Где она применяется?
52. Предмет Web-программирования, его особенности. Различия в программировании на стороне клиента и сервера. Инструменты и технологии программирования.
53. Приведите примеры HTTP-заголовков HTTP-запроса и HTTP-ответа.
54. Протокол HTTP. Структура запросов и ответов.
55. Работа с базой данных. JDBC
56. Работа с базой данных. OR – Mapping. JPA API
57. стек технологий J2EE. Основные возможности и компоненты.
58. Технология AJAX и ее компоненты. Особенности фоновых запросов.
59. Технология AJAX. Методы обмена данными с серверными сценариями.
60. Технология AJAX. Методы обработки событий в документе.
61. Технология AJAX. Форматы передаваемых данных.
62. Транзакции - ACID, уровни изоляции и блокировки. Алгоритм «оптимистических блокировок». Дайте характеристику физического уровня модели OSI.
63. Чем CGI отличается от ISAPI?
64. Чем отличается модель DARPA (DoD) от модели OSI? Как вы думаете, почему?
65. Чем отличаются симметричные алгоритмы шифрования от асимметричных?
66. Что представляет собой трехуровневая архитектура ANSI-SPARC; каково ее назначение?
67. Что такое RFC? В файлах какого формата издаются RFC?

68. Что такое браузер?
69. Что такое веб-приложение?
70. Что такое веб-сервер?
71. Что такое виртуальный хостинг?
72. Что такое заголовки HTTP-сообщения и для чего они нужны?
73. Что такое коммутаторы? Опишите принцип их работы..
74. Что такое метод HTTP-запроса?
75. Что такое методы шифрования и дешифрования сообщений? Для чего они применяются?
76. Что такое протокол? Какие протоколы входят в состав стека TCP/IP.
77. Что такое пул приложения?
78. Что такое сетевые протоколы? Опишите типы протоколов.
79. Что такое статусный код HTTP-ответа?
80. Что такое тело HTTP-сообщения?
81. Что такое технология ATM?
82. Что такое хостинг? Опишите принцип его работы и предоставляемые сервисы.

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

Порядок и методика проведения промежуточной аттестации и текущего контроля

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания теста для оценки теоретических знаний;
- текущий 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 проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся 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 обучающимися практических навыков исследования на аппаратуре.

Тестовый контроль усвоения лекционного материала выполняются в виде короткого письменного или устного 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 обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися в рамках текущего контроля 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 обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Основы информационной безопасности»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Тестовый контроль)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	10	40
Экзамен	100		

Теоретический блок оценивается по результатам тестового контроля. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

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

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена. Экзамен проводится по расписанию промежуточной аттестации в устном виде по экзаменационным билетам.

Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

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 И.о.зав. кафедрой «ИБ» _____ А.Г. Жуковский. «___» _____ 20__ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 3 Дисциплина: Администрирование средств защиты информации в компьютерных системах и сетях		
Билет №1 1. История развития средств безопасности информационных систем. 2. Связь аппаратной и программной составляющих. «___» _____ 20__ г. Доцент, к.т.н., с.н.с. _____ Ткачук Е.О.		

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 по дисциплине «Администрирование средств защиты информации в компьютерных системах и сетях»

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-1.2; Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень 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 в среднем составляет 35 % заданий.

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

Высокий уровень 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 равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ОПК-1.2

Способен администрировать средства защиты информации в компьютерных системах и сетях

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

№ задания	Тексты заданий
1	Какая команда позволяет проверить наличие соединения между хостами?: 1. netstat 2. nbtstat 3. ping 4. ipconfig
2	Какая команда позволяет отобразить активные сетевые подключения и порты соединений? 1. netstat 2. route 3. ping 4. ipconfig
3	Какая команда позволяет отображать и изменять таблицу маршрутизации? 1. netstat 2. route 3. ping 3. ipconfig
4	Какая команда позволяет отобразить список существующих сетевых адаптеров? 1. netstat 2. nbtstat 3. ping 4. ipconfig
5	Какая команда позволяет сделать общим сетевым ресурсом с именем MyCommonName локальную папку D:\USERS\MyFolder? 1. net share MyCommonName=D:\USERS\MyFolder 2. net use MyCommonName=D:\USERS\MyFolder 3. net config MyCommonName=D:\USERS\MyFolder 4. net name MyCommonName disk=D:\USERS\MyFolder
6	Запишите команду, позволяющую подключить в качестве сетевого диска J: общую папку CommonDir

№ задания	Тексты заданий
	на компьютере US112-SRV. 1. net share J: \\US112-SRV\CommonDir 2. net use J: \\US112-SRV\CommonDir 3. net config J: \\US112-SRV folder=CommonDir 4. net name disk=J: server=US112-SRV folder=CommonDir
7	Какая служба Windows позволяет использовать общие ресурсы сети (папки и принтеры)? 1. SERVER 2. WORKSTATION 3. NetBIOS 4. CONNECTION
8	Какая команда позволяет вывести список запущенных процессов на компьютере \\admin-is? 1. tasklist /s \\admin-is 2. taskenum \\admin-is 3. commandlist /computer \\admin-is 4. processid /s \\admin-is
9	Запишите команду, создающую группу MyOwnGroup с одноименной учетной записью в качестве локальной группы в домене tc.rosnou.ru. 1. dsadd group "OU=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU" -samid MyOwnGroup -scope l 2. dsadd group "CN=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU" -samid MyOwnGroup -scope l 3. dsadd group "OU= MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU" -samid MyOwnGroup -localgroup 4. dsadd group "CN= MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU" -samid MyOwnGroup -group=local
10	Какая команда позволяет, установить пароль p@ssw0rd для пользователя с учетной записью NewUSER в домене TC. 1. NET PASSWORD p@ssw0rd /USER NewUSER /DOMAIN 2. NET USER NewUSER /PASSWORD p@ssw0rd /DOMAIN TC 3. NET USER NewUSER p@ssw0rd /DOMAIN 4. NET /USER NewUSER p@ssw0rd /DOMAIN TC

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

№ задания	Тексты заданий
11	Установите соответствие между названиями сетевых протоколов и их функциями: 1. SSH 2. http. 3. ftp А. Протокол передачи файлов по сети. Б. Сетевой протокол для безопасного доступа к удалённым компьютерам и серверам. В. Протокол прикладного уровня, разработанный для обмена данными между клиентом и сервером.
12	Установите соответствие между основными типами угроз, характерных для компьютерных систем, и примерами их реализации: 1. Логические угрозы; 2. Физические угрозы; 3. Неправильное управление доступом; А. Несанкционированный доступ к оборудованию. Б. Вредоносный код, встроенный в приложения. В. Назначение избыточных прав пользователям.
13	Установите соответствие между типами мероприятий по защите компьютерных систем и их описаниями: 1. Технические мероприятия; 2. Процедурные (или административные) мероприятия;

№ задания	Тексты заданий
	3. Физические мероприятия; А. Применение организационных мер и совокупности средств, создающих препятствие для проникновения или доступа неуполномоченных физических лиц к защищаемой; Б. Обеспечение защиты (конфиденциальности, целостности, доступности) содержащейся в ОС информации при помощи программных и технических средств; В. Разработка и применение стандартов, требований, регламентов и прочих нормативных документов, направленных на обеспечение защиты, содержащейся в системе информации;
14	Установите соответствие между возможными рисками в компьютерной системе и их последствиями: 1. Потеря целостности; 2. Потеря конфиденциальности; 3. Потеря функциональности, А. Манипуляции с данными; Б. Несанкционированное получение информации; В. Потеря или разрушение данных.

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Установите правильную последовательность этапов контроля доступа пользователя при входе в компьютерную систему на основе операционной системы семейства Unix: 1) Пользователь вводит пароль, который преобразуется в хеш и сравнивается с хешем, содержащимся в специальном хранилище 2) Пользователь вводит символьное имя (логин), для которого проверяется его наличие в специализированном хранилище 3) Реализуется доступ пользователя к объектам системы в соответствии с правами доступа к ним на основе дискреционной модели 4) Происходит присвоение пользователю числовых идентификаторов UID и GID
16	Установите правильную последовательность этапов доступа пользователя к компьютерной системе: 1). Авторизация, 2). Идентификация 3). Аутентификация 4). Расшифрование зашифрованных данных
17	Установите правильную последовательность этапов процесса реагирования на инциденты в компьютерной системе: 1. Идентификация, 2. Ликвидация, 3. Улучшение, 4. Подготовка, 5. Возвращение к работе, 6. Сдерживание.

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	В комплекс программно-технических средств и организационных (процедурных) решений по защите информации от _____ к компьютерной системе входят: - криптографическая подсистема - подсистема управления доступом - подсистема обеспечения целостности - подсистема регистрации и учета.
19	_____ обеспечивает такие состояния безопасности информации в компьютерной системе, как конфиденциальность, целостность, идентифицируемость
20	Меры по достижению требуемого уровня _____ в компьютерной системе от несанкционированного доступа сформулированы руководящем документе «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Система оценивания выполнения тестовых заданий по компетенции ОПК-1.2

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	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

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 решаемым в работе задачам.

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 промежуточной аттестации знаний обучающихся.

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 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.

Достижение целей эффективной подготовки обучающихся в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава. 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. Обязательным компонентом самостоятельной работы обучающихся является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий, учебно-методических материалов, образцов техники
- содержать материал, углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему обучающиеся должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений,

техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков;
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала раздела 4 необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего:
Модуль 1 – 19 часа		
1	Оптоволоконные кабельные системы. Изучение методов терминирования и сплайсирования оптоволоконных кабельных систем.	5
2	Создание элементов структурированной кабельной системы. Горизонтальная подсистема. Подсистема рабочего места.	5
3	Изучение топологии сетевых систем. Способы соединения, диагностики и тестирования кабельной системы на основе витой пары.	4
4	Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	5
Модуль 2 – 19 часа		
9	Способы реализации протоколов IEEE 802.1xx. Настройка VLAN коммутатора.	5
10	Изучение управления портом коммутатора 100-Base Ethernet. Задание параметров порта. Проверка состояния.	5
11	Изучение вопросов адресации устройств. Конфигурация протокола ARP.	4
12	Изучение протоколов маршрутизации. Конфигурация протокола RIP.	5

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.