

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

2026 г.

Рабочая программа дисциплины

Б1.О.36.03 Безопасность компьютерных сетей

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	ОФО	
	ЗЕ	Часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/7
Контактная работа, в том числе (по семестрам, курсам):		96/7
Лекции		32/7
Лабораторных работ		32/7
Практических занятий		32/7
Семинаров		
Самостоятельная работа		48/7
Контроль		36/7
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)		1/7

Кандидат технических наук, доцент Манин А.А.

«Безопасность компьютерных сетей»

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427.

одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026 г., и
утвержденного директором СКФ МТУСИ 31.03 2026 г.

Информационная безопасность

Протокол от «28» 04 2026 г. № 9

И.О.Зав. кафедрой _____ Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины «Безопасность компьютерных сетей» является формирование у обучаемых знаний в области обеспечения безопасности компьютерных сетей и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях.

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:

- понятия целостность, конфиденциальность, доступность как основных характеристик защищенности информации;
- модели политик информационной безопасности в компьютерных сетях;
- средства обеспечения защищенного доступа к сетевому оборудованию;
- протоколы защищенного информационного обмена в компьютерных сетях;
- основные способы организации безопасного соединения через незащищенные общедоступные сети.

Уметь:

- классифицировать и оценивать угрозы информационной безопасности в компьютерных сетях;
- проводить работы по администрированию средств защиты информации в компьютерных сетях;
- использовать механизмы аутентификации и авторизации в компьютерных сетях;
- конфигурировать встроенные в сетевое оборудование средства защиты;
- проводить работы по разграничению прав доступа пользователей к сетевым ресурсам;

Владеть:

- основными понятиями, связанными с обеспечением безопасности компьютерных сетей;
- навыками работы по конфигурированию средств защиты компьютерных сетей.

ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

Знать

- методы анализа и оценки защищенности компьютерных систем;
- этапы и процедуры аудита информационной безопасности защищенных компьютерных систем;
- особенности комплексного подхода к обеспечению информационной безопасности организации.

Уметь

- разрабатывать и применять методики оценки защищенности программно-аппаратных средств защиты информации компьютерных систем;
- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.

Владеть

- методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищенных компьютерных систем нормативным требованиям по защите информации; -

владеть методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации;
- технологией разработки комплекта нормативно-методического обеспечения комплексной защиты информации на предприятии.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Безопасность компьютерных сетей» является логическим продолжением дисциплин: Б1.О.27 «Основы информационной безопасности», Б1.О.29 «Методы и средства криптографической защиты информации», Б1.О.41 «Сетевые технологии», знание которых в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Безопасность компьютерных сетей» базируется также на знаниях, приобретенных из дисциплин: Б1.О.20 «Физика», Б1.О.07 «Иностранный язык», Б1.В.06 «Введение в профессию».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.33 «Программно-аппаратные средства защиты информации», Б1.О.36.04 «Безопасность систем баз данных», Б1.В.02 «Комплексное обеспечение защиты информации», Б1.О.36.05 «Методы оценки безопасности компьютерных систем (Аудит компьютерных систем», Б1.О.36.06 «Администрирование средств защиты информации в компьютерных системах и сетях».

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 96 аудиторных часов, 48 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компет енции	УМИО
Курс 4, Семестр 7					
Модуль 1. Методы и средства защиты элементов сетей от НСД. (30+30) часов					
1.1	Лекция 1. МОДЕЛИ ПОЛИТИК БЕЗОПАСНОСТИ 1. Общие понятия. 2. Дискреционная модель. 3. Мандатная модель. 4. Ролевая модель. 5. Результативная кибербезопасность	Л1.	2	ОПК-1.2 ОПК-1.4	Л1.1
1.2	Лекция 2. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ	Л2.	2	ОПК-1.2 ОПК-1.4	Л1.1

	1. Защита консольного доступа. 2. Протоколы удаленного доступа к сетевому оборудованию. 3. Защита удаленного доступа.				
1.3	Лекция 3. ИСПОЛЬЗОВАНИЕ AAA-СЕРВЕРА ДЛЯ ЗАЩИТЫ УДАЛЕННОГО ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ 1. Основные понятия. 2. Протоколы RADIUS и TACACS+. 3. Принципы конфигурирования маршрутизаторов для работы с протоколом TACACS+. 4. Логирование сетевых событий.	ЛЗ.	2	ОПК-1.2 ОПК-1.4	Л1.1
1.4	Практическое занятие 1 Конфигурирование защиты консольного доступа	ПЗ1	2	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
1.5	Практическое занятие 2 Конфигурирование защиты удаленного доступа	ПЗ2	2	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
1.6	Практическое занятие 3 Конфигурирование защиты удаленного доступа с использованием AAA- и Syslog-серверов	ПЗ3	2	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
1.7	Лекция 4. 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.	Л4	6	ОПК-1.2 ОПК-1.4	Л1.1
1.8	Лекция 5. СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IDS/IPS) 1. Принцип работы системы обнаружения вторжений (IDS). 2. Принцип работы системы предотвращения вторжений (IPS). 3. Зеркалирование портов для контроля трафика. 4. Сигнатуры атак. 5. Принципы конфигурирования IPS.	Л5	2	ОПК-1.2 ОПК-1.4	Л1.1
1.9	Практическое занятие 4 Конфигурирование межсетевого экрана с пакетной фильтрацией	ПЗ4	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
1.10	Практическое занятие 5 Конфигурирование межсетевого экрана с сохранением состояний	ПЗ5	2	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
1.11	Практическое занятие 6 Конфигурирование межсетевого экрана Zone-Based Policy Firewall	ПЗ6	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
1.12	Требования нормативных документов и технических регламентов к защищенным сетям связи.	СРС	30	ОПК-1.2 ОПК-1.4	Л1.1 Л2.1

	Технические характеристики аппаратных межсетевых экранов различных производителей. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Обеспечение защиты беспроводного сетевого оборудования. Механизмы комплексной защиты сетей электросвязи. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.				Л2.2 Л2.3
Модуль 2 Защита локальных и корпоративных сетей от НСД. (66+18) часов					
2.1	Лекция 6. ТЕХНОЛОГИИ ЛОКАЛЬНЫХ И КОРПОРАТИВНЫХ СЕТЕЙ 1. Структура стека TCP/IP. 2. Семейство технологий Ethernet (IEEE 802.3). 3. Коммутаторы Ethernet. 4. Технологии виртуальных локальных сетей (VLAN). 5. Исключение петель в локальных сетях (протокол STP). 6. Принципы маршрутизации. 7. Протоколы динамической маршрутизации. 8. Вспомогательные протоколы и службы стека TCP/IP (DNS, DHCP, ARP).	Л6	10	ОПК-1.2 ОПК-1.4	Л1.1
2.2	Лекция 7. АРХИТЕКТУРА ЗАЩИЩЕННЫХ СЕТЕЙ 1. Уровни сетевой защиты. 2. Структура защищенной сети. 3. Методы и средства повышения сетевой доступности.	Л7	2	ОПК-1.2 ОПК-1.4	Л1.1
2.3	Лекция 8. ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ЛОКАЛЬНЫХ И КОРПОРАТИВНЫХ СЕТЕЙ 1. Технология трансляции сетевых адресов (NAT). 2. Защита от атак на VLAN. 3. Защита от атак на протокол STP. 4. Использование функции Port Security. 5. Защита от атак на протоколы DHCP и ARP.	Л8	4	ОПК-1.2 ОПК-1.4	Л1.1
2.4	Лекция 9. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) 1. Технологии туннелирования. Протокол GRE. 2. Архитектура IPSec. 3. Протокол AH. 4. Протокол ESP. 5. Принципы конфигурирования VPN IPSec.	Л9	2	ОПК-1.2 ОПК-1.4	Л1.1
2.5	Лабораторная работа 1 Исследование коммутаторов Ethernet	ЛР1	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3

2.6	Практическое занятие 7 Конфигурирование статической маршрутизации	ПЗ7	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.7	Лабораторная работа 2 Исследование процессов динамической маршрутизации	ЛР2	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.8	Практическое занятие 8 Построение и конфигурирование локальной сети	ПЗ8	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.9	Практическое занятие 9 Построение локальной сети с комплексной защитой	ПЗ9	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.10	Лабораторная работа 3 Исследование локальной сети с повышенной сетевой доступностью	ЛР3	6	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.11	Практическое занятие 11 Конфигурирование Site-to-Site VPN	ПЗ10	4	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.12	Лабораторная работа 4 Исследование аппаратно-программного межсетевого экрана D-Link с функционалом VPN	ЛР4	6	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.13	Лабораторная работа 5 Исследование защищенной корпоративной сети на базе оборудования Cisco Systems	ЛР5	6	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.14	Лабораторная работа 6 Исследование средств защиты сетей на базе программного комплекса GNS3	ЛР6	6	ОПК-1.2 ОПК-1.4	Л2.1, Л2.2, Л2.3
2.15	Механизмы защиты корпоративной сети от DoS-атак. Угрозы информационно-программному обеспечению, характерные только для корпоративных и локальных сетей. Механизмы защиты корпоративных и локальных сетей от компьютерных вирусов. Области применения технологий VPN второго уровня (L2). Организационные мероприятия по комплексной защите корпоративных и локальных сетей. Анализ моделей нарушителя; угрозы сетевой безопасности и их классификация. Методы и средства обеспечения доступности и целостности информации в корпоративных и локальных сетях.	СРС	18	ОПК-1.2 ОПК-1.4	Л2.1 Л2.2 Л2.3
	Экзамен		36	ОПК-1.2 ОПК-1.4	Л1.1 Л2.1 Л2.2 Л2.3
Итого – 180 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	Манин А.А.	Методы и средства защиты компьютерной информации Учебное пособие.	Ростов-на-Дону: СКФ МТУСИ, 2019. – 177 с.	Э1
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Манин А.А., Сосновский И.А.	Системы коммутации. Принципы и технологии пакетной коммутации. Учебное пособие. Изд-е 3-е, перераб. и доп.	Ростов-на-Дону: СКФ МТУСИ, 2019. – 245 с.	Э2
Л2.2	Мэйволд, Э.-	Безопасность сетей : учебное пособие	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 571 с.	Э3
Л2.3	Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М -	Технологии защиты информации в компьютерных сетях. Учебное пособие	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 368 с.	Э4
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Манин А.А.	Системы коммутации. Методические указания для проведения практических занятий	Ростов-на-Дону: СКФ МТУСИ, 2024. – 64 с.	Э4
5.2. Электронные образовательные ресурсы				
Э1	https://elib.mtuci.ru/view.php?book_id=170036			
Э2	https://elib.mtuci.ru/view.php?book_id=170038			
Э3	https://www.iprbookshop.ru/146327.html			
Э4	https://www.iprbookshop.ru/146404.html			
Э5	https://elib.mtuci.ru/view.php?book_id=169995			
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	Электронный ресурс http://www.securitylab.ru/			
5.3.5	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.6	Профессиональная база данных: Федеральный центр информационно-образовательных			

ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)		
5.4. Программное обеспечение		
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:		
П.1	ОС Windows	Лицензионное ПО.
П.2	ОС Linux	Свободно распространяемое ПО.
П.3	Cisco Packet Tracer	Свободно распространяемое ПО.
П.4	ОС Cisco IOS	ПО поставляется вместе с сетевым оборудованием.
П.5	GNS-3	Свободно распространяемое ПО.

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Цифровых систем коммутации и сетей связи»
2	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, прочитывать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Безопасность компьютерных сетей Б1.О.36.03» 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, 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
ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях		
Знать:		
Понятия целостность, конфиденциальность, доступность как основных характеристик защищенности информации; Модели политик информационной безопасности в компьютерных сетях; Средства обеспечения защищенного доступа к сетевому оборудованию.	Контрольная работа 1	Модуль 1 0÷20 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-10 «Хорошо» - 11-15 «Отлично» - 16-20
Протоколы защищенного информационного обмена в компьютерных сетях; Основные способы организации безопасного соединения через незащищенные общедоступные сети.	Контрольная работа 2	Модуль 2 0÷20 «Неудовлетворительно» - 0-5 «Удовлетворительно» - 6-10 «Хорошо» - 11-15 «Отлично» - 16-20
Уметь:		
Использовать механизмы аутентификации и авторизации в компьютерных сетях; Конфигурировать встроенные в сетевое оборудование средства защиты; Проводить работы по разграничению прав доступа пользователей к сетевым ресурсам.	Практическое занятие 1-3	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Классифицировать и оценивать угрозы информационной безопасности в компьютерных сетях; Конфигурировать встроенные в сетевое оборудование средства защиты.	Практическое занятие 4-6	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Проводить работы по администрированию средств защиты информации в компьютерных сетях.	Лабораторная работа 1-2	Модуль 2 0÷3 за каждую ЛР «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Практическое занятие 7-8	Модуль 2 0÷3 за каждое ПЗ «Неудовлетворительно» - 0

		«Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Владеть:		
Основными понятиями, связанными с обеспечением безопасности компьютерных сетей; навыками работы по конфигурированию средств защиты компьютерных сетей.	Практическое занятие 9-10	Модуль 2 0÷3 за каждое ПЗ «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Основными понятиями, связанными с обеспечением безопасности компьютерных сетей; навыками работы по конфигурированию средств защиты компьютерных сетей.	Лабораторная работа 3-6	Модуль 2 0÷3 за каждую ЛР «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями		
Знать:		
методы анализа и оценки защищённости компьютерных систем; этапы и процедуры аудита информационной безопасности защищённых компьютерных систем; особенности комплексного подхода к обеспечению информационной безопасности организации;	Контрольная работа 1	Модуль 1 0÷20 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-10 «Хорошо» - 11-15 «Отлично» - 16-20
	Контрольная работа 2	Модуль 2 0÷20 «Неудовлетворительно» - 0-5 «Удовлетворительно» - 6-10 «Хорошо» - 11-15 «Отлично» - 16-20
Уметь:		
разрабатывать и применять методики оценки защищённости программно-аппаратных средств защиты информации компьютерных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	Практическое занятие 1-6	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 9	Модуль 2 0÷3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Владеть:		
методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых компьютерных систем нормативным требованиям по защите информации; владеть методиками проверки защищённости объектов информатизации на соответствие	Практическое занятие 1	Модуль 1 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое	Модуль 1

требованиям безопасности информации; технологией разработки комплекта нормативно-методического обеспечения комплексной защиты информации на предприятии	занятие 2-3	0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 4-6	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 10	Модуль 2 0÷3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	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 14 часов лекционных занятий, 16 часов практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 20. За выполненное и защищенное практическое занятие обучающийся получает максимум 5 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ОПК-1.2, ОПК-1.4):

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 консольного доступа к сетевому оборудованию.

Задание (ОПК-1.2, ОПК-1.4).

Используя программные продукты (Cisco Packet Tracer или GNS3) или реальное оборудование, подключиться к консольному порту устройства (коммутатора или маршрутизатора). Создать пароль для входа в привилегированный режим, используя параметр **secret**. Создать три учетные записи с разными уровнями привилегий, используя функцию AAA. При создании учетных записей использовать логин **<фамилия в английской транскрипции>** и **№ учетной записи**. Проверить работоспособность системы аутентификации и авторизации по локальной базе пользователей.

Практическое занятие 2. Конфигурирование удаленного доступа к сетевому оборудованию.

Задание (ОПК-1.2, ОПК-1.4).

– Используя консольный порт, создать в локальной базе маршрутизатора одну учетную запись с первым уровнем привилегий. Создать пароль входа в привилегированный режим, используя параметр **secret**. Проверить работоспособность системы аутентификации.

– Подключить к одному из Ethernet-портов маршрутизатора рабочую станцию, произведя необходимые настройки (IP-адреса порта маршрутизатора и рабочей станции). Осуществить удаленное подключение к маршрутизатору с использованием протокола Telnet. Проверить работоспособность системы аутентификации.

– Сконфигурировать маршрутизатор для работы с протоколом SSH, исключив возможность использования протокола Telnet. Используя SSH-клиент, осуществить удаленное подключение к маршрутизатору с использованием протокола SSH. Проверить работоспособность системы аутентификации.

Практическое занятие 3. Конфигурирование защиты удаленного доступа с использованием AAA- и Syslog-серверов.

Задание (ОПК-1.2, ОПК-1.4).

– Построить сеть, включающую в себя AAA-сервер, Syslog-сервер, маршрутизатор и управляющий ПК.

– Настроить IP-адресацию.

- Сконфигурировать серверы, создать учетные записи.
- Проверить работоспособность системы аутентификации.

Практическое занятие 4. Конфигурирование межсетевого экрана с пакетной фильтрацией.

Задание (**ОПК-1.2, ОПК-1.4**).

- В Cisco Packet Tracer создать сеть, состоящую из пяти подсетей. В одной из подсетей установить два сервера, один из которых должен быть сконфигурирован как FTP, а другой – как WEB-сервер.
- Всем компьютерам подсети 192.169.X.0 (где X – номер обучающегося в списке группы) предоставить полный доступ ко всем серверам.
- Всем компьютерам подсети 192.169.X+1.0 предоставить доступ только к FTP-серверу по протоколу FTP.
- Всем компьютерам подсети 192.169.X+2.0 предоставить доступ только к WEB-серверу.
- Компьютерам оставшейся подсети запретить доступ к внешним ресурсам.

Практическое занятие 5. Конфигурирование межсетевого экрана с сохранением состояний.

Задание (**ОПК-1.2, ОПК-1.4**).

- Используя Cisco Packet Tracer, построить сеть, показанную на рисунке 3.4. Произвести конфигурирование сетевых устройств для обеспечения доступа всех серверов из внутренней сети.
- Убедиться в возможности доступа во внутреннюю сеть извне с использованием произвольного протокола.
- Настроить инспектирование TCP-трафика и сконфигурировать список доступа. Убедиться в доступности серверов из внутренней сети и недоступности ресурсов внутренней сети извне.

Практическое занятие 6. Конфигурирование межсетевого экрана Zone-Based Policy Firewall.

Задание (**ОПК-1.2, ОПК-1.4**).

- Собрать сеть, показанную на рисунке 3.1, настроить адресацию по следующим исходным данным:
 - внутренняя сеть – 192.168.X.0;
 - демилитаризованная зона – 192.168.X+10.0;
 - внешняя сеть – 213.80.X.0.
- Проверить связность сети.
- Сконфигурировать на маршрутизаторе межсетевой экран ZBFW, обеспечивающий выполнение следующих правил:
 - из внутренней сети разрешены все запросы к внешней сети;
 - к демилитаризованной зоне разрешены запросы из внутренней сети по протоколам Telnet и SSH и только с адресов, принадлежащих внутренней сети;
 - из внешней сети запросы во внутреннюю сеть запрещены;
 - из внешней сети запросы в демилитаризованную зону разрешены только по протоколу HTTP.
- Проверить работоспособность межсетевого экрана.

Модуль 2: (50 баллов):

Модуль содержит 18 часов лекционных занятий, 16 часов практических занятий и 32 часа лабораторных занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 20. За выполненную и защищенную лабораторную работу и практическое занятие обучающийся получает максимум 3 балла. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 2 (ОПК-1.2, ОПК-1.4):

1. Структура стека TCP/IP.
2. Коммутаторы Ethernet.
3. Технологии виртуальных локальных сетей (VLAN).
4. Исключение петель в локальных сетях (протокол STP).
5. Протоколы динамической маршрутизации.
6. Вспомогательные протоколы и службы стека TCP/IP (DNS, DHCP, ARP).
7. Уровни сетевой защиты.
8. Структура защищенной сети.
9. Методы и средства повышения сетевой доступности.
10. Статический NAT.
11. Динамический NAT.
12. NAT с применением маскардинга.
13. Защита от атак на VLAN.
14. Защита от атак на протокол STP.
15. Использование функции Port Security.
16. Защита от атак на протоколы DHCP и ARP.
17. Определение и классификация VPN.
18. Протоколы VPN, реализуемые на втором уровне модели OSI.
19. Протоколы VPN, реализуемые на третьем уровне модели OSI.
20. Протоколы туннелирования.
21. Протоколы IPSec.
22. Dos и DDos-атаки.
23. Системы обнаружения вторжений (IDS).
24. Системы предотвращения вторжений (IPS).
25. Классификация компьютерных вирусов.
26. Применение антивирусного ПО на шлюзах корпоративной сети.
27. Классификация корпоративного антивирусного ПО.
28. Протоколы RPTP, L2TP, L2PW.
29. Сравнительный анализ протоколов второго уровня.
30. Применение протоколов второго уровня в системе Site-to-Site.
31. Применение протоколов второго уровня в системе Remote VPN.
32. Организационные мероприятия по комплексной защите корпоративной сети.

Лабораторная работа 1. Исследование коммутаторов Ethernet.

Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть, состоящую из коммутатора и четырех ПК, назначить IP-адреса.
- Исследовать процесс заполнения адресной таблицы в процессе обучения коммутатора.
- Создать на коммутаторе две VLAN.
- Дополнить сеть еще одним коммутатором, создать на нем такие же VLAN.
- Соединить коммутаторы между собой с использованием Trunk-порта.
- Исследовать передачу трафика.

Практическое занятие 7. Конфигурирование статической маршрутизации.
Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть, состоящую из трех подсетей, назначить IP-адреса.
- Сконфигурировать на центральном маршрутизаторе статические маршруты.
- Сконфигурировать на остальных маршрутизаторах маршруты по умолчанию.
- Исследовать передачу трафика.

Лабораторная работа 2. Исследование процессов динамической маршрутизации.
Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть, состоящую из четырех подсетей, назначить IP-адреса.
- Сконфигурировать на маршрутизаторах протокол RIP.
- Исследовать передачу трафика.
- Сконфигурировать на маршрутизаторах протокол OSPF.
- Исследовать передачу трафика.
- Сконфигурировать на маршрутизаторах протокол EIGRP.
- Исследовать передачу трафика.

Практическое занятие 8. Построение и конфигурирование локальной сети.
Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в соответствии со своими исходными данными.
- Сконфигурировать DNS-сервер.
- Сконфигурировать на граничном маршрутизаторе службу DHCP.
- Сконфигурировать на граничном маршрутизаторе NAT.
- Исследовать передачу трафика.

Практическое занятие 9. Построение локальной сети с комплексной защитой.
Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в соответствии со своими исходными данными.
- Сконфигурировать на центральном коммутаторе службу DHCP.
- Сконфигурировать на граничном маршрутизаторе NAT.
- Разделить сеть на пользовательские и серверные VLAN.
- Разграничить права доступа пользователей к внутренним серверам.
- Сконфигурировать Port Security.
- Проверить работоспособность системы защиты.

Лабораторная работа 3. Исследование локальной сети с повышенной сетевой доступностью.

Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в соответствии со своими исходными данными.
- Сконфигурировать на маршрутизаторах протокол VRRP.
- Исследовать передачу трафика.

Практическое занятие 10. Конфигурирование Site-to-Site VPN.

Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в соответствии со своими исходными данными.
- Сконфигурировать на граничных маршрутизаторах VPN с заданными параметрами.
- Проверить работоспособность VPN-канала.

Лабораторная работа 4. Исследование аппаратно-программного межсетевого экрана D-Link с функционалом VPN.

Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в соответствии со своими исходными данными.
- Сконфигурировать на МСЭ фильтрацию трафика и VPN.
- Исследовать передачу трафика.

Лабораторная работа 5. Исследование защищенной корпоративной сети на базе оборудования Cisco Systems.

Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в соответствии со своими исходными данными.
- Сконфигурировать на центральном коммутаторе службу DHCP.
- Сконфигурировать на граничном маршрутизаторе NAT.
- Разделить сеть на пользовательские и серверные VLAN.
- Разграничить права доступа пользователей к внутренним серверам.
- Сконфигурировать Port Security.
- Исследовать передачу трафика.

Лабораторная работа 6. Исследование средств защиты сетей на базе программного комплекса GNS3.

Задание (ОПК-1.2, ОПК-1.4).

- Собрать сеть в среде GNS3 в соответствии со своими исходными данными.
- Сконфигурировать на центральном коммутаторе службу DHCP.
- Сконфигурировать на граничном маршрутизаторе NAT.
- Разделить сеть на пользовательские и серверные VLAN.
- Разграничить права доступа пользователей к внутренним серверам.
- Сконфигурировать Port Security.
- Исследовать передачу трафика.

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Методы и средства защиты компьютерной информации» (ОПК-1.2, ОПК-1.4) (промежуточная аттестация):

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. Структура стека TCP/IP.

29. Коммутаторы Ethernet.

30. Технологии виртуальных локальных сетей (VLAN).

31. Исключение петель в локальных сетях (протокол STP).

32. Протоколы динамической маршрутизации.

33. Вспомогательные протоколы и службы стека TCP/IP (DNS, DHCP, ARP).

34. Уровни сетевой защиты.

35. Структура защищенной сети.

36. Методы и средства повышения сетевой доступности.

37. Статический NAT.

38. Динамический NAT.

39. NAT с применением маскардинга.

40. Защита от атак на VLAN.

41. Защита от атак на протокол STP.

42. Использование функции Port Security.

43. Защита от атак на протоколы DHCP и ARP.

44. Определение и классификация VPN.

45. Протоколы VPN, реализуемые на втором уровне модели OSI.

46. Протоколы VPN, реализуемые на третьем уровне модели OSI.

47. Протоколы туннелирования.

48. Протоколы IPSec.

49. Dos и DDos-атаки.

50. Системы обнаружения вторжений (IDS).

51. Системы предотвращения вторжений (IPS).

52. Классификация компьютерных вирусов.

53. Применение антивирусного ПО на шлюзах корпоративной сети.

54. Классификация корпоративного антивирусного ПО.

55. Протоколы RPTP, L2TP, L2PW.

56. Сравнительный анализ протоколов второго уровня.

57. Применение протоколов второго уровня в системе Site-to-Site.

58. Применение протоколов второго уровня в системе Remote VPN.

59. Организационные мероприятия по комплексной защите корпоративной сети.

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

Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы 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 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 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 обучающимся 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 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 обучающимся 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.

Для получения зачета обучающемуся достаточно набрать от 41 и более баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по блокам модулей дисциплины

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	20	30=5+5+5+5+5+5
Модуль 2	50	20	30=3+3+3+3+3+3+3+3+3+3
Экзамен	100		100

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

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: 4 Дисциплина: Безопасность компьютерных сетей		
Билет №7 1. Межсетевые экраны с пакетной фильтрацией. 2. Протокол маршрутизации RIP. Доцент, к.т.н. _____ Манин А.А. «___» _____ 20__ г.		

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

4 Вопросы для тестирования (ОПК-1.2, ОПК-1.4)

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций:

ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях;

ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

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 ОПК-1.2 равно 20, по компетенции ОПК-1.4 равно 20. Всего 40 заданий

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	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 ____ 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

№ задания	Тексты заданий
	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 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.

№ задания	Тексты заданий
	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 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	Технология _____ VPN предназначена для передачи конфиденциальной информации между корпоративными/локальными сетями по общедоступной сети
19	_____ в модели политики информационной безопасности сетевые ресурсы, дисковое пространство, серверы, сегменты сети
20	Атаки, связанные с перехватом данных из других виртуальных локальных сетей называются _____

Система оценивания выполнения тестовых заданий по компетенции ОПК-1.2, формируемой дисциплиной Безопасность компьютерных сетей Б1.О.36.03

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.

ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

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	Протокол RADIUS позволяет 1. передавать все данные в зашифрованном виде 2. передавать в зашифрованном виде только пароль 3. передавать все данные в незашифрованном виде
2	Протокол TACACS+ позволяет 1. передавать все данные в зашифрованном виде 2. передавать в зашифрованном виде только пароль 3. передавать все данные в незашифрованном виде
3	Авторизация пользователя предполагает 1. установление личности 2. определение действий, доступных пользователю 3. определение возможности физического доступа к оборудованию
4	Межсетевые экраны с пакетной фильтрацией анализируют 1. происхождение трафика 2. сетевые адреса, содержащиеся в пакете 3. данные протоколов прикладного уровня
5	Межсетевые экраны с сохранением состояний анализируют 1. состояние открытых TCP-соединений 2. данные протоколов прикладного уровня 3. MAC-адреса отправителя и получателя
6	Стандартный список доступа анализирует поступивший пакет по следующим критериям 1. сетевой адрес источника 2. сетевой адрес получателя 3. сетевые адреса источника и получателя
7	Расширенный список доступа анализирует поступивший пакет по следующим критериям 1. сетевые адреса источника и получателя 2. протоколы транспортного и прикладного уровня 3. MAC-адреса отправителя и получателя 4. состояние открытых TCP-соединений
8	При создании зон безопасности на МСЭ ZBFW 1. между зонами трафик по умолчанию запрещен 2. между зонами трафик по умолчанию разрешен 3. между зонами трафик инспектируется 4. трафик разрешен только к зоне DMZ
9	Для фильтрации трафика в МСЭ ZBFW используются критерии: 1. с третьего по седьмой уровень модели OSI 2. с четвертого по седьмой уровень модели OSI 3. с пятого по седьмой уровень модели OSI
10	Между различными сегментами корпоративной сети создается защищенный канал 1. Site-to-Site VPN 2. Remote VPN 3. Access VPN

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

№ задания	Тексты заданий
11	При конфигурировании зонального межсетевого экрана создаются: 1. Политики межсетевого экранирования; 2. Классовые карты; 3. Зоны безопасности. Расставьте в соответствии их определениям: А. Группы интерфейсов, трафик между которыми по умолчанию запрещен; Б. Трафик с определенными критериями; В. Действия над трафиком.
12	При создании учетной записи на сетевом оборудовании могут быть назначены следующие привилегии: 1. Уровень 0. 2. Уровень 1. 3. Уровни 2 - 14. 4. Уровень 15. Расставьте в соответствии с возможностями уровней: А. Возможность выполнения всех команд. Б. Возможность выполнения команд, указанных в явном виде. В. Возможность выполнения команд пользовательского режима. Г. Возможность выполнения четырех базовых команд.
13	Для защиты от вредоносного трафика могут использоваться следующие средства: 1. Межсетевые экраны следующего поколения (NGFW) 2. Системы обнаружения вторжений (IDS) 3. Системы предотвращения вторжений (IPS) Расставьте в соответствии с их описанием: А. Зеркалируют внешний трафик для его дальнейшей проверки Б. Проверяет проходящий через него трафик на наличие аномалий В. Принимает решение о пропуске или блокировке входящего трафика
14	В VPN на основе туннелирования используются термины: 1. Транспортирующий протокол. 2. Транспортируемый протокол. 3. Протокол инкапсуляции. Поставьте в соответствие их определению А. протокол, описывающие правила инкапсуляции данных транспортируемого протокола в пакет транспортирующего протокола. Б. протокол, на базе которого данные доставляются через некоторую транзитную сеть (например, через Интернет). В. протокол, в котором представлены данные, которые необходимо передать через туннель.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности
Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Определить правильный порядок реализации этапов результативной кибербезопасности 1. Активное противодействие киберугрозам; 2. Определение недопустимых событий; 3. Проведение киберучений.
16	Установить правильный порядок действий при серверной аутентификации: 1. Маршрутизатор обращается к AAA-серверу и передает ему учетные данные пользователя; 2. Пользователь пытается подключиться к сетевому устройству, вводя свои учетные данные; 3. AAA-сервер ищет в своей базе соответствующую учетную запись (Authentication) и определяет уровень привилегий (Authorization); 4. AAA-сервер фиксирует данное событие (Accounting); 5. AAA-сервер пересылает маршрутизатору соответствующую информацию (успешность аутентификации, уровень привилегий); 6. Маршрутизатор открывает доступ пользователя к оборудованию с учетом уровня привилегий.

№ задания	Тексты заданий
17	Расставьте в правильном порядке этапы конфигурирования зонального межсетевого экрана: 1. Определение пар зон (zone pair). 2. Определение зон (zone). 3. Определение политики (действий) в отношении выбранного трафика (policy map). 4. Выделение интересующего трафика (class map). 5. Применение политики к парам зон (service policy).

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	_____ предназначен для преобразования частных адресов в общедоступные при передаче пакетов из внутренней сети во внешнюю и для обратного преобразования при приеме
19	_____ – порт, за которым располагается DHCP-сервер, и с которого сообщения протокола DHCP передаются на оконечные устройства.
20	_____ – определение того, что разрешено делать аутентифицированному пользователю.

Система оценивания выполнения тестовых заданий по компетенции ОПК-1.4, формируемой дисциплиной Безопасность компьютерных сетей Б1.О.36.03

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, промежуточного и итогового контроля 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.

1. Для подготовки и выполнения практических занятий используется методическая разработка: Манин А.А. Методические указания для проведения практических занятий по дисциплине «Безопасность компьютерных сетей».

2. Для подготовки и выполнения лабораторных работ используется методическая разработка: Манин А.А. Методические указания для проведения лабораторных работ по дисциплине «Безопасность компьютерных сетей».

3. Методические рекомендации для обучающихся по самостоятельной работе

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 занятий, 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.

Обучающимся очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1 рабочей программы, рекомендуется соблюдать последовательность их изучения, представленную в таблице.

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.	Неделя	Кол. час.
Модуль 1 – 30 часов			
1	Требования нормативных документов и технических регламентов к защищенным сетям связи 1.1. Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 1.2. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.	1-2	4
2	Технические характеристики аппаратных межсетевых экранов различных производителей 2.1 МСЭ Cisco. 2.2 МСЭ D-Link. 2.3 МСЭ Huawei. 2.4 МСЭ TP-link. 2.5 Отечественные решения.	3-4	4
3	Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения	5	4
4	Обеспечение защиты беспроводного сетевого оборудования 3.1. Процедуры аутентификации и авторизации в сетях IEEE 802.11. 3.2. Защита беспроводных устройств от НСД.	6	4
5	Механизмы комплексной защиты сетей электросвязи 4.1. Оформление политики безопасности сети. 4.2. Управление паролями. 4.3. Управление правами доступа. 4.4 Мониторинг активности пользователей. 4.5 Мониторинг уязвимости ПО. 4.6 Управление обновлениями ПО и ОС.	7	4

6	Положение о лицензировании деятельности по технической защите конфиденциальной информации.	8	4
7	Обеспечение сохранения коммерческой тайны предприятия	9	2
8	Каталог обобщенных мероприятий по защите конфиденциальной информации.	10	4
Модуль 2 – 18 часов			
9	Механизмы защиты корпоративной сети от DoS-атак 7.1 Dos и DDos-атаки. 7.2 Системы обнаружения вторжений (IDS). 7.3 Системы предотвращения вторжений (IPS).	11-12	4
	Угрозы информационно-программному обеспечению, характерные только для корпоративных и локальных сетей	13	2
10	Механизмы защиты корпоративных и локальных сетей от компьютерных вирусов 8.1 Классификация компьютерных вирусов. 8.2 Применение антивирусного ПО на шлюзах корпоративной сети. 8.3 Классификация корпоративного антивирусного ПО.	14	4
11	Области применения технологий VPN второго уровня (L2) 9.1 Протоколы PPTP, L2TP, L2PW. 9.2 Сравнительный анализ протоколов второго уровня. 9.3. Применение протоколов второго уровня в системе Site-to-Site. 9.4 Применение протоколов второго уровня в системе Remote VPN.	15	2
12	Организационные мероприятия по комплексной защите корпоративной сети	16	2
13	Анализ моделей нарушителя; угрозы сетевой безопасности и их классификация	16	2
14	Методы и средства обеспечения доступности и целостности информации в корпоративных и локальных сетях 14.1 Резервное копирование данных. 14.2 Использование RAID-массивов 14.3 Особенности использования различных хэш-функций	16	2

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