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 УВР
_____ А.Г. Жуковский
«_29_» _____08_____ 2022 г.

Безопасность компьютерных сетей Б1.О.31
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	180/6 сем		
Контактная работа, в том числе (по семестрам, курсам):		90/6 сем		
Лекции		20/6 сем		
Лабораторных работ		24/6 сем		
Практических занятий		46/6 сем		
Семинаров				
Самостоятельная работа		90/6 сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)		1/6 сем		
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/6 сем		

Программу составил:
Доцент кафедры ИТСС, к.т.н., доцент Манин А.А.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Безопасность компьютерных сетей»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. №1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «29» 08 2022 г. № 1

Зав. кафедрой _____ В.И. Юхнов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

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 выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)

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.

ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях

Знать:

- принципы функционирования аппаратно-программных средств защиты информации в компьютерных сетях;
- принципы внедрения средств защиты информации в компьютерные сети;
- принципы мониторинга инцидентов с использованием аппаратно-программных средств защиты информации в компьютерных сетях.

Уметь:

- проводить работы по конфигурированию и администрированию аппаратно-программных средств защиты информации в компьютерных сетях.

Владеть:

- навыками конфигурирования защищенного удаленного доступа; - навыками конфигурирования средств аутентификации; - навыками конфигурирования аппаратно-программных средств межсетевого экранирования; - навыками конфигурирования аппаратно-программных средств для организации виртуальных частных сетей.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Безопасность компьютерных сетей» является логическим продолжением дисциплин Б1.О.1 «Основы информационной безопасности», Б1.О.25 «Методы и средства криптографической защиты информации», Б1.В.06 «Сетевые технологии (Интернет-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.06 «Физика», Б1.О.07 «Иностранный язык», Б1.В.01 «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 «Безопасность систем баз данных», Б1.О.37 «Комплексное обеспечение защиты информации», Б1.О.39 «Методы оценки безопасности компьютерных систем (Аудит компьютерных систем», Б1.О.40 «Администрирование средств защиты информации в компьютерных системах и сетях».

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 90 аудиторных часов, 90 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 6					
Модуль 1. Методы и средства защиты элементов сетей от НСД. (34+40) часов					
1.1	Лекция 1. МОДЕЛИ ПОЛИТИК БЕЗОПАСНОСТИ 1. Общие понятия. 2. Дискреционная модель. 3. Мандатная модель. 4. Ролевая модель.	Л1.	2	ОПК-1.2 ПК-2	Л1.1
1.2	Лекция 2. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ 1. Защита консольного доступа. 2. Протоколы удаленного доступа к сетевому оборудованию. 3. Защита удаленного доступа.	Л2.	2	ОПК-1.2 ПК-2	Л1.1
1.3	Лекция 3. ИСПОЛЬЗОВАНИЕ AAA-СЕРВЕРА ДЛЯ ЗАЩИТЫ	Л3.	2	ОПК-1.2	Л1.1

	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.			ПК-2	
1.4	Практическое занятие 1 Конфигурирование защиты консольного доступа	ПЗ1	4	ОПК-1.2 ПК-2	Л3.1
1.5	Практическое занятие 2 Конфигурирование защиты удаленного доступа	ПЗ2	4	ОПК-1.2 ПК-2	Л3.1
1.6	Практическое занятие 3 Конфигурирование защиты удаленного доступа с использованием AAA- и Syslog-серверов	ПЗ3	4	ОПК-1.2 ПК-2	Л3.1
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).	Л4	4	ОПК-1.2 ПК-2	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 ПК-2	Л1.1
1.9	Практическое занятие 4 Конфигурирование межсетевого экрана с пакетной фильтрацией	ПЗ4	4	ОПК-1.2 ПК-2	Л3.1
1.10	Практическое занятие 5 Конфигурирование межсетевого экрана с сохранением состояний	ПЗ5	2	ОПК-1.2 ПК-2	Л3.1
1.11	Практическое занятие 6 Конфигурирование межсетевого экрана Zone-Based Policy Firewall	ПЗ6	4	ОПК-1.2 ПК-2	Л3.1
1.12	Требования нормативных документов и технических регламентов к защищенным сетям связи. 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.	СРС	40	ОПК-1.2 ПК-2	Л1.1 Л2.1 Л2.2 Л2.3

	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.				
Модуль 2 Защита локальных и корпоративных сетей от НСД. (56+50) 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	4	ОПК-1.2 ПК-2	Л1.1
2.2	Лекция 7. 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.	Л7	2	ОПК-1.2 ПК-2	Л1.1
2.3	Лекция 8. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) 1. Технологии туннелирования. Протокол GRE. 2. Архитектура IPSec. 3. Протокол AH. 4. Протокол ESP. 5. Принципы конфигурирования VPN IPSec.	Л6	2	ОПК-1.2 ПК-2	Л1.1
2.4	Лабораторная работа 1 Исследование коммутаторов Ethernet	ЛР1	4	ОПК-1.2 ПК-2	Л3.2
2.5	Практическое занятие 7 Конфигурирование статической маршрутизации	ПЗ7	6	ОПК-1.2 ПК-2	Л3.1
2.6	Лабораторная работа 2 Исследование процессов динамической маршрутизации	ЛР2	4	ОПК-1.2 ПК-2	Л3.2
2.7	Практическое занятие 8 Построение и конфигурирование локальной сети	ПЗ8	6	ОПК-1.2 ПК-2	Л3.1
2.8	Практическое занятие 9 Построение локальной сети с комплексной защитой	ПЗ9	6	ОПК-1.2 ПК-2	Л3.1

2.9	Практическое занятие 10 Конфигурирование Site-to-Site VPN	ПЗ10	6	ОПК-1.2 ПК-2	Л3.1
2.10	Лабораторная работа 3 Исследование аппаратно-программного межсетевого экрана D-Link с функционалом VPN	ЛР3	6	ОПК-1.2 ПК-2	Л3.2
2.11	Лабораторная работа 4 Исследование защищенной корпоративной сети на базе оборудования Cisco Systems	ЛР4	6	ОПК-1.2 ПК-2	Л3.2
2.12	Лабораторная работа 5 Исследование средств защиты сетей на базе программного комплекса GNS3	ЛР5	4	ОПК-1.2 ПК-2	Л3.2
2.13	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	50	ОПК-1.2 ПК-2	Л2.1 Л2.2 Л2.3
	Экзамен			ОПК-1.2 ПК-2	Л1.1 Л1.2 Л1.3
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.	Безопасность компьютерных сетей. Учебное пособие.	Ростов-на-Дону: СКФ МТУСИ, 2022.	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.	Э2
Л2.2	-	Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 “Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации”.		Э3
Л2.3	-	ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения		Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Манин А.А.	Методическое пособие для практических занятий по дисциплине «Методы и средства защиты компьютерной информации».	Ростов-на-Дону: СКФ МТУСИ, 2022.	Э5
Л3.2	Манин А.А.	Методическое пособие для лабораторных работ по дисциплине «Методы и средства защиты компьютерной информации».	Ростов-на-Дону: СКФ МТУСИ, 2019.	Э6

5.2. Электронные образовательные ресурсы	
Э1	http://www.skf-mtusi.ru
Э2	http://www.skf-mtusi.ru
Э3	https://www.garant.ru/products/ipo/prime/doc/92632/
Э4	http://docs.cntd.ru/document/1200044726
Э5	http://www.skf-mtusi.ru
Э6	http://www.skf-mtusi.ru

5.3. Программное обеспечение		
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	Компьютерный класс с установленным пакетом Cisco Packet Tracer
2	Программно-аппаратный комплекс «Инфокоммуникационные сети»
3	Компьютерный класс с установленным пакетом GNS-3
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет.

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов 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 студентов 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 студентов 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 студенты 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 студентов 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 баз) 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.

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 7.1.

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам 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 – 40 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	6
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	6
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	6

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	6
6	**Положение о лицензировании деятельности по технической защите конфиденциальной информации.**	8	4
7	**Обеспечение сохранения коммерческой тайны предприятия**	9	4
8	**Каталог обобщенных мероприятий по защите конфиденциальной информации.**	10	4
Модуль 2 – 50 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	8
	Угрозы информационно-программному обеспечению, характерные только для корпоративных и локальных сетей	13	4
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	10
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	8
12	**Организационные мероприятия по комплексной защите корпоративной сети**	16	6
13	**Анализ моделей нарушителя; угрозы сетевой безопасности и их классификация**	16	6
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	8

Дополнения и изменения в рабочей программе