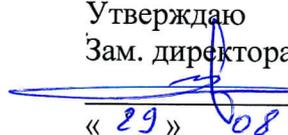


МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР

А.Г. Жуковский
« 29 » 08 2022 г.

**Администрирование средств защиты информации в компьютерных системах
и сетях Б1.О.40**
рабочая программа дисциплины

Кафедра: Информатика и вычислительная техника
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	144/8сем		
Контактная работа, в том числе (по семестрам, курсам):		72/8сем		
Лекции		24/8сем		
Лабораторных работ		24/8сем		
Практических занятий		24/8сем		
Семинаров				
Самостоятельная работа		72/8сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)		1/8сем		
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/8сем		

Программу составил:

Доцент кафедры ИВТ, к.т.н., с.н.с. Ткачук Е.О.

Рецензент:

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

Рабочая программа дисциплины

«Администрирование средств защиты информации в компьютерных системах и сетях»

разработана в соответствии с ФГОС ВО:

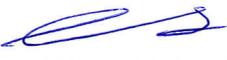
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МГУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МГУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «29» 08 2022г. №1

Зав. кафедрой  С.В. Соколов

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

Утверждаю

Зам. директора по УВР _____

«__» _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Информатика и вычислительная техника»

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

«Информатика и вычислительная техника»

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

«Информатика и вычислительная техника»

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

«Информатика и вычислительная техника»

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

Зав. кафедрой _____

1. Цели изучения дисциплины

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

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у 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-1.1: Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
Знать:
<ul style="list-style-type: none">- виды политик управления доступом и информационными потоками в компьютерных сетях;- источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению;- состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;- методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.
Уметь:
<ul style="list-style-type: none">- оценивать угрозы безопасности информации в компьютерных сетях;- настраивать правила фильтрации пакетов в компьютерных сетях;обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;- конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях;- выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;- проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях.
Владеть:
<ul style="list-style-type: none">- принципами работы и правилами эксплуатации эксплуатируемых программно-аппаратных средств защиты информации- программно-аппаратными средствами и методами защиты информации в компьютерных сетях- нормативными правовыми актами в области защиты информации- руководящими и методическими документами уполномоченных федеральных органов - исполнительной власти по защите информации- организационными мерами по защите информации
ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях
Знать:
<ul style="list-style-type: none">- принципы построения компьютерных сетей- стек сетевых протоколов операционных систем- стек протоколов сетевого оборудования

- порядок реализации методов и средств межсетевого экранирования принципы функционирования сетевых протоколов, включающих криптографические алгоритмы
Уметь:
- производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях - использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации;
Владеть:
- источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению - состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях - методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации - принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Администрирование средств защиты информации в компьютерных системах и сетях» является логическим продолжением дисциплины Б1.О.11 «Основы информационной безопасности», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Администрирование средств защиты информации в компьютерных системах и сетях» базируется также на знаниях, приобретенных из дисциплин: Б1.О.06 «Физика», Б1.О.07 «Иностранный язык», Б1.О.12 «Введение в информационные технологии».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б2.В.03(Пд) Производственная (преддипломная) практика; Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы

4. Структура и содержание дисциплины

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

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 2					
Модуль 1. Общие принципы администрирования информационных систем. (36+24) часов					
1.1	Лекция 1. АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ. Вводные положения. Функции администратора системы. Состав служб администратора системы и их назначение. Требования к специалистам. Стандарты работы ИС и стандартизирующие организации. Объекты администрирования и модели управления. Модель сетевого управления ISO. Модель FCAPS. Модель ITIL. Модель TMN. Модель e ГОМ. Модель RPC	Л1.	4	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. АДМИНИСТРИРОВАНИЕ КАБЕЛЬНЫХ СИСТЕМ И СЕТЕВЫХ СИСТЕМ Администрирование кабельных систем. Понятие о средах передачи. Кабельные системы передачи данных. Стандарты и задачи администрирования кабельных систем. Управление коммутаторами. Вопросы проектирования сети. Понятие систем сетевого администрирования.	Л2.	4	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. СРЕДСТВА АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ. АДМИНИСТРИРОВАНИЕ ФАЙЛОВЫХ СИСТЕМ. Средства администрирования операционных систем. Администрирование файловых систем. Параметры ядра ОС. Установка ОС. Подсистема ввода/вывода и способы организации дискового пространства. Технология RAID. Файловые системы Интернет.	Л3.	4	ОПК-1.1	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие 1. Администрирование адресации компьютеров в локальной сети. MAC адрес, IP адрес, понятие URL. Маска подсети. Выдача задания на курсовую работу.	ПЗ1	6	ОПК-1.1	Л3.1
1.5	Практическое занятие 2. Программное обеспечение администрирования сетей ЭВМ Программное обеспечение вычислительных сетей; Возможности сетевых операционных сред. Анализ корректности архитектуры сети Ethernet в соответствии с индивидуальным вариантом.	ПЗ2	6	ОПК-1.1	Л3.1
1.6	Лабораторная работа 1. Способы подключения оптоволоконных мультиплексоров Изучение способов подключения оптоволоконных	ЛР1	6	ОПК-1.1	Л3.1

	мультиплексоров и проверки соединения оптоволоконных систем.				
1.7	Лабораторная работа № 2. Способы соединения сетевых устройств. Способы соединения сетевых устройств. Подключение рабочих станций к коммутатору и установка параметров ОС. Проверка соединения	ЛР2	6	ОПК-1.1	
1.8	1.Оптоволоконные кабельные системы. Изучение методов терминирования и сплайсирования оптоволоконных кабельных систем. 2.Создание элементов структурированной кабельной системы. Горизонтальная подсистема. Подсистема рабочего места. 3.Изучение топологии сетевых систем. Способы соединения, диагностики и тестирования кабельной системы на основе витой пары. 4. Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	СРС	24	ОПК-1.1	Л1.1 Л1.2 Л1.3
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях (36+24)					
2.1	Лекция 4. АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ. Администрирование баз данных. Средства СУБД. Администрирование данных. Инсталляция СУБД. Параметры ядра СУБД и параметры ввода/вывода. Средство мониторинга и сбора статистики. Средства защиты от несанкционированного доступа. Способы восстановления и реорганизации БД. Стратегии администратора БД.	ЛЗ	4	ОПК-1.2	Л1.1 Л1.2 Л1.3
2.2	Лекция 5. АДМИНИСТРИРОВАНИЕ ПРОЦЕССА ПОИСКА И ДИАГНОСТИКИ ОШИБОК. Администрирование процесса поиска и диагностики ошибок. 12 задач управления при обнаружении ошибки ИС. Базовая модель поиска ошибки. Стратегия определения ошибок. Средства сбора и поиска ошибок администратора системы. Метрика работы ИС. Примеры диагностики ошибок для технологии Ethernet и для среды протоколов TCP/IP. Предупреждение ошибок и решение проблем в среде протоколов TCP/IP.	Л5	4	ОПК-1.2	Л1.1 Л1.2 Л1.3
2.3	Лекция 6. АДМИНИСТРИРОВАНИЕ ПРОЦЕССА КОНФИГУРАЦИИ, ПРОЦЕССА УЧЕТА И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Администрирование процесса конфигурации. Задачи и проблемы конфигурации. Оценки эффективности конфигурации с точки зрения бизнеса. Администрирование процесса учета и обеспечения информационной безопасности. Задачи учета. Защита от	Л6	4	ОПК-1.2	Л1.1 Л1.2 Л1.3

	угроз безопасности. Средства, мероприятия и нормы обеспечения безопасности. Пример реализации защиты от НСД для ИС. Пример реализации средств безопасности для сетевой подсистемы ИС.				
2.4	Практическое занятие 3 Канальный уровень модели OSI: Протокол LLC. Реализация LLC. Протоколы канального уровня.	ЛР5	6	ОПК-1.2	Л3.1
2.5	Практическое занятие 4. Диагностика Ethernet и TCP/IP Средства диагностики Ethernet и TCP/IP. Утилита PING. Диагностика Ethernet и TCP/IP. Утилита Traceroute. Изучение средств отладки соединений	ЛР6	6	ОПК-1.2	Л3.1
2.6	Лабораторная работа № 3 Администрирование адресации устройств Изучение вопросов адресации устройств. Конфигурация протокола ARP	ЛР3	6	ОПК-1.2	
2.7	Лабораторная работа № 4 Администрирование коммутации пакетов в сетях Способы управления коммутатором. Задание базовых параметров ОС коммутатора. Изучение методов защиты от несанкционированного доступа.	ЛР4	6	ОПК-1.2	
2.8	1.Способы реализации протоколов IEEE 802.1xx. Настройка VLAN коммутатора. 2.Изучение управления портом коммутатора 100-Base Ethernet. Задание параметров порта. Проверка состояния. 3.Изучение вопросов адресации устройств. Конфигурация протокола ARP. 4.Изучение протоколов маршрутизации. Конфигурация протокола RIP.	СРС	24	ОПК-1.2	Л1.1 Л1.2 Л1.3
Модуль 3 Курсовая работа					
3.1	Курсовая работа	КР	24	ОПК-1.2	Л1.1
	Экзамен			ОПК-1.1, ОПК-1.2	Л1.1 Л1.2 Л1.3
Итого – 144 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Гаспариан, М. С. Н. Лихачева.	Информационные системы и технологии : учебное пособие.	Москва : Евразийский открытый институт, 2011. — 370 с.	Э1
Л1.2	Семакин И.Г. Хеннер Е.К.-	Информационные системы и модели	М.: БИНОМ. Лаборатория знаний, 2012.- 71 с.	Э2
Л1.3	Фомин, Д. В.	Информационная безопасность: учебник	Москва : Ай Пи Ар Медиа, 2022. — 222 с.	Э3
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Гатчин Ю.А., Климова Е.В.	Введение в комплексную защиту объектов информатизации	СПб.: Университет ИТМО, 2011. — 112 с. — 2227-8397. —	Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Нестеров С.А.	Основы информационной безопасности [Электронный ресурс]: учебное пособие/— Электрон. текстовые данные.	СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с.	Э5
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/10680.html			
Э2	http://www.ip1-bookshop.ru/6473			
Э3	https://www.iprbookshop.ru/118876.html			
Э4	http://www.iprbookshop.ru/65808.html			
Э5	https://www.iprbookshop.ru/43960			
5.3. Программное обеспечение				
П.1	1. AVAST Free Antivirus	Антивирусное ПО. Свободное, условно свободное или триал-версии.		
	2. AVG AntiVirus Free			
	3. Dr.Web Antivirus			
	4. Антивирус Касперского			
	5. ESET NOD32 Антивирус			
	6. AVZ Antivirus			
	7. Avira Free Antivirus			
	8. Norton AntiVirus			
	9. McAfee Antivirus			
	10. Emsisoft Anti-Malware			
	11. BullGuard Antivirus			
	12. Protector Plus Antivirus			
	13. Panda Antivirus			

	<ul style="list-style-type: none"> 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus 	
II.2	<ul style="list-style-type: none"> 1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files 	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
II.3	<ul style="list-style-type: none"> 1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition 	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
II.4	<ul style="list-style-type: none"> 1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Paragon Rescue Kit 7. Wise Data Recovery 8. Puran File Recovery 9. O&O DiskRecovery 10. Tenorshare Any Data Recovery 11. Power Data Recovery 12. GetDataBack 13. Recover My Files 14. R-Undelete 15. Handy Recovery 	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

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

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

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

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

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

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.	Часов всего: 24	Неделя
Модуль 1 – 24 часа			
1	Оптоволоконные кабельные системы. Изучение методов терминирования и сплайсирования оптоволоконных кабельных систем.	6	1,2
2	Создание элементов структурированной кабельной системы. Горизонтальная подсистема. Подсистема рабочего места.	6	3,4
3	Изучение топологии сетевых систем. Способы соединения, диагностики и тестирования кабельной системы на основе витой пары.	6	5,6
4	Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	6	7,8
Модуль 2 – 24 часа			
9	Способы реализации протоколов IEEE 802.1xx. Настройка VLAN коммутатора.	6	9,10
10	Изучение управления портом коммутатора 100-Base Ethernet. Задание параметров порта. Проверка состояния.	6	11, 12
11	Изучение вопросов адресации устройств. Конфигурация протокола ARP.	6	12, 13
12	Изучение протоколов маршрутизации. Конфигурация протокола RIP.	6	13, 14

Дополнения и изменения в рабочей программе