

Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.12 Инфокоммуникационные системы и их
информационная защита

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

25.05.03 Техническая эксплуатация транспортного радиооборудования

Направленность (профиль)

25.05.03.31 Информационно-телекоммуникационные системы на
транспорте и их информационная защита

Форма обучения

очная

Год набора

2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

канд.техн.наук, Доцент, Черников Дмитрий Юрьевич

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Подготовка специалистов готовых к самостоятельной работе в области администрирования локальных сетей и иных областях, смежных с вопросами администрирования локальных сетей.

Дисциплина является базовой и входит в дисциплины специализации.

1.2 Задачи изучения дисциплины

Изучение: принципов администрирования различных локальных инфокоммуникационных сетей при помощи различных протоколов, алгоритмов их работы, выполняемых задач, технических средств, вопросов управления и проектирования локальных сетей и их элементов, а так же других вопросов необходимых для достижения поставленной цели.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-2: Способен к проектированию РТС и РЭС	
ПК-2.1: Разбирается в цифровых технологиях, включая системы САПР разного уровня, для проектирования, конструирования, анализа данных, подготовки документации, построения математических моделей, в том числе методами 3D-моделирования	технологии и средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающие выполнение требований нормативных правовых актов и методических документов в области информационной безопасности методы и технологии обеспечения эффективной защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующей требованиям нормативных правовых актов и методических документов в области информационной безопасности выбирать технологии и средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающие при этом выполнение требований нормативных правовых актов и методических документов в области информационной безопасности выбирать наиболее эффективные методы и технологии обеспечения эффективной защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующей требованиям нормативных правовых актов и методических документов в области информационной безопасности навыками выбора наиболее эффективных методов, технологий и средств обеспечения эффективной

	<p>защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующих выполнения требований нормативных правовых актов и методических документов в области информационной безопасности</p> <p>навыками выбора наиболее эффективных методов, технологий и средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающих при этом выполнение требований нормативных правовых актов и методических документов в области информационной безопасности</p>
<p>ПК-2.2: Рассчитывает проектные параметры и формирует проектный облик РТС и РЭС</p>	<p>методы, технологии и средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающие выполнение требований нормативных правовых актов и методических документов в области информационной безопасности</p> <p>порядок оценки уровня защищённости, в том числе возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации</p> <p>выбирать наиболее эффективные методы, технологии и средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающие при этом выполнение требований нормативных правовых актов и методических документов в области информационной безопасности</p> <p>реализовывать на практике порядок оценки уровня защищённости, в том числе возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации</p> <p>навыками проектных параметров</p> <p>навыками реализации на практике средств оценки уровня защищённости, в том числе возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации</p>

<p>ПК-2.3: Разрабатывает технические задания и эскизные проекты РТС и РЭС</p>	<p>состав документов для подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации технологии, средства и порядок оценки уровня защищённости, в том числе возможностей средств</p>
	<p>технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации использовать на практике порядок подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации реализовывать на практике технологии и порядок оценки уровня защищённости навыками определения порядка подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации навыками реализации на практике технологий и средств оценки уровня защищённости, в том числе возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации</p>
<p>ПК-3: Способен к реализации программ экспериментальных исследований</p>	

<p>ПК-3.1: Понимает технологии автоматической обработки информации</p>	<p>состав документов для подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации форму документов для подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающие выполнение требований нормативных правовых актов и методических документов в области информационной безопасности реализовывать на практике возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации использовать на практике состав и порядок подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации навыками реализации на практике методов, технологий, средств и порядка оценки уровня защищённости, в том числе возможностей средств</p>
	<p>технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации навыками определения состава, формы и порядка подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации</p>

<p>ПК-3.2: Использует измерительное оборудование для настройки составных частей радиоэлектронных систем</p>	<p>методы, технологии средства и порядок оценки уровня защищённости, в том числе возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации состав, форму и порядок подготовки заключений по итогам аттестации телекоммуникационных систем требованиям защиты информации; реализовывать на практике методы, технологии, средства и порядок оценки уровня защищённости, в том числе возможностей средств технической разведки, применительно к системам связи, управления и объектам информатизации при проведении аттестации телекоммуникационных систем по требованиям защиты информации; определять состав, форму и порядок подготовки заключений по итогам аттестации</p>
	<p>телекоммуникационных систем требованиям защиты информации. выбирать рациональный порядок обеспечения защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующей требованиям нормативных правовых актов и методических документов в области информационной безопасности навыками выбора средств обеспечения эффективной защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующих выполнения требований нормативных правовых актов и методических документов в области информационной безопасности навыками выбора средств закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающих при этом выполнение требований нормативных правовых актов и методических документов в области информационной безопасности</p>

<p>ПК-3.3: Осуществляет мониторинг технического состояния радиоэлектронных систем по основным показателям</p>	<p>порядок обеспечения эффективной защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующей требованиям нормативных правовых актов и методических документов в области информационной безопасности</p> <p>технологии обеспечения эффективной защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующей требованиям нормативных правовых актов и методических документов в области</p>
	<p>информационной безопасности</p> <p>выбирать рациональные средства закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающие при этом выполнение требований нормативных правовых актов и методических документов в области информационной безопасности</p> <p>выбирать технологии обеспечения эффективной защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующей требованиям нормативных правовых актов и методических документов в области информационной безопасности</p> <p>навыками выбора технологий и средств обеспечения защиты информационных ресурсов, компьютерных сетей и систем беспроводной связи, соответствующих выполнения требований нормативных правовых актов и методических документов в области информационной безопасности</p> <p>навыками выбора технологий и средств закрытия каналов перехвата речевой информации в телекоммуникационных системах, обеспечивающих при этом выполнение требований нормативных правовых актов и методических документов в области информационной безопасности</p>

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
Контактная работа с преподавателем:	1,5 (54)	
занятия лекционного типа	1 (36)	
лабораторные работы	0,5 (18)	
Самостоятельная работа обучающихся:	1,5 (54)	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	
Промежуточная аттестация (Экзамен)	1 (36)	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Введение. Повторение протокола IP									
	1. Введение. Повторение протокола IP	1							
	2. Введение. Повторение протокола IP							2	
2. Протоколы динамической конфигурации: DHCP (Dynamically Host Configuration Protocol) и DNS (Domain Name System)									
	1. Протоколы динамической конфигурации	2							
	2. Составление различных MSC-сценариев протокола DHCP.					1			
	3. Протоколы динамической конфигурации					1			
	4. Протоколы динамической конфигурации							3	
3. Общие сведения о частных виртуальных сетях VPN (Virtual Private Network)									
	1. Общие сведения о частных виртуальных сетях VPN (Virtual Private Network)	2							
	2. Общие сведения о частных виртуальных сетях VPN (Virtual Private Network)					1			

3. Общие сведения о частных виртуальных сетях VPN (Virtual Private Network)								3	
4. Протоколы организации VPN на канальном уровне: PPTP, L2F, L2TP									
1. Протоколы организации VPN на канальном уровне: PPTP, L2F, L2TP	2								
2. Протоколы организации VPN на канальном уровне: PPTP, L2F, L2TP						1			
3. Протоколы организации VPN на канальном уровне: PPTP, L2F, L2TP								4	
5. Протокол организации VPN на сетевом уровне: IPSecurity (Internet Protocol Security)									
1. Протокол организации VPN на сетевом уровне: IPSecurity (Internet Protocol Security)	2								
2. Исследование работы протокола AH и ESP. Составления структуры пакета при одновременном использовании протоколов AH и ESP, IPSecurity						1			
3. Протокол организации VPN на сетевом уровне: IPSecurity (Internet Protocol Security)						1			
4. Протокол организации VPN на сетевом уровне: IPSecurity (Internet Protocol Security)								4	
6. Протокол организации VPN сетей на сеансовом уровне: TLS/SSL (Transport Layer Security/Socket Security Layer)									
1. Протокол организации VPN сетей на сеансовом уровне: TLS/SSL (Transport Layer Security/Socket Security Layer)	2								
2. Протокол организации VPN сетей на сеансовом уровне: TLS/SSL (Transport Layer Security/Socket Security Layer)						1			

3. Протокол организации VPN сетей на сеансовом уровне: TLS/SSL (Transport Layer Security/Socket Security Layer)							4	
7. Управление ключевой информацией: Инфраструктура открытых ключей (Public Key Infrastructure, PKI)								
1. Правила построения структуры PKI. Построение структуры PKI согласно индивидуальным заданиям. Имитация алгоритма работы полученной PKI.					1			
2. Управление ключевой информацией: Инфраструктура открытых ключей (Public Key Infrastructure, PKI)							2	
3. Управление ключевой информацией: Инфраструктура открытых ключей (Public Key Infrastructure, PKI)	2							
8. Криптографическая защита информации								
1. Криптографическая защита информации	2							
2. Криптографическая защита информации					1			
3. Криптографическая защита информации							4	
4. Законодательные требования в области VPN сетей. Проектирование VPN	2							
9. Законодательные требования в области VPN сетей. Проектирование VPN								
1. Проектирование VPN					1			
2. Законодательные требования в области VPN сетей. Проектирование VPN							4	
10. Мониторинг и качество обслуживания в сетях VPN								
1. Мониторинг и качество обслуживания в сетях VPN	2							
2. Мониторинг и качество обслуживания в сетях VPN							2	
11. Протокол NTTP								
1. Протокол NTTP	2							
2. Изучение работы протокола NTTP в среде GNS3					2			

3. Протокол HTTP							4	
12. Протокол FTP								
1. Протокол FTP	4							
2. Протокол FTP					1			
3. Изучение работы протокола FTP в среде GNS3					1			
4. Протокол FTP							4	
13. Почтовый сервер SMTP								
1. Почтовый сервер SMTP	4							
2. Сервер SMTP					1			
3. Изучение работы протокола SMTP в среде GNS3					1			
4. Почтовый сервер SMTP							4	
14. Базы данных. Язык структурированных запросов SQL (Structured query language)								
1. Базы данных. Язык структурированных запросов SQL (Structured query language)	5							
2. Язык структурированных запросов SQL (Structured query language)					1			
3. Элементы Администрирования СУБД в среде MySQL							4	
15. Протокол OpenFlow								
1. Протокол OpenFlow	2							
2. Протокол OpenFlow					1			
3. Протокол OpenFlow							6	
4.								
Всего	36				18		54	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для вузов по направлению 552800- "Информатика и вычислительная техника" и по специальностям 220100- "Вычислительные машины, комплексы, системы и сети", 220200 - "Автоматизированные системы обработки информации и управления" и 220400- "Программное обеспечение вычислительной техники и автоматизированных систем"(Москва: Питер).
2. Кузин А. В., Кузин Д. А. Компьютерные сети: Учебное пособие(Москва: Издательство "ФОРУМ").
3. Айвалиотис Д. Администрирование сервера NGINX: учебное пособие (Москва: ДМК-пресс).
4. Росляков А. В., Ваняшин С. В., Самсонов М. Ю., Шибаета И. В., Чечнева И. А., Росляков А. В. Сети следующего поколения NGN (Москва: Эко-Трендз).
5. Култыгин О.П. Администрирование баз данных. СУБД MS SQL Server: учебное пособие(Москва: МФПА).
6. Беленькая М. Н., Малиновский С. Т., Яковенко Н. В. Администрирование в информационных системах: учебное пособие (Москва: Горячая линия - Телеком).
7. Росляков А. В. Зарубежные и отечественные платформы сетей NGN (Москва: Горячая линия-Телеком).
8. Запечников С. В., Милославская Н. Г., Толстой А. И. Основы построения виртуальных частных сетей: Учебное пособие для вузов(Москва: Горячая линия-Телеком).
9. Гаипов К. Э., Турбов А. Ю. Технологии локальных инфокоммуникационных сетей: учеб.-метод. пособие для лаб. и самостоят. работ [для студентов напр. 210400.62 «Телекоммуникации» и спец. «210406.65» «Сети связи и системы коммутации»](Красноярск: СФУ).
10. Гаипов К. Э., Турбов А. Ю. Системы документальной электросвязи: учеб.-метод. пособие для курс. проектирования [для студентов спец. 210406.65 «Сети связи и системы коммутации»](Красноярск: СФУ).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Среда моделирования GNS3.
2. Среда моделирования VirtualBox.
3. Анализатор пакетов WireShark.
4. Cisco VPN Client.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Сайт библиотеки СФУ. Режим доступа: <http://bik.sfu-kras.ru/>
2. Электронный каталог библиотеки СФУ. Режим доступа: <http://catalog.sfu-kras.ru/>
3. Google Scholar. Режим доступа: <http://scholar.google.com>
4. Электронные базы научных статей по выбору студента

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория с 10 рабочими местами, оснащенными ЭВМ для выполнения практических работ и проведения лекционных занятий.