МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И НАНОЭЛЕКТРОНИКИ

Утверждено:
на заседании кафедры
протокол от №5 от 17.02.2021

Зав. кафедрой  / Салихов Р.Б

Согласовано:
Председатель УМК физико-технического института

 / Балапанов М.Х.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ СВЯЗИ

часть, формируемая участниками образовательных отношений

Дисциплины по выбору Б1.В.ДВ.4

(Указать часть (обязательная часть или часть, формируемая участниками образовательных отношений, факультатив))

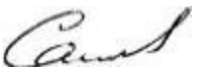
программа бакалавриата

Направление подготовки (специальность)
11.03.02 Инфокоммуникационные технологии и системы связи ,
(указывается код и наименование направления подготовки (специальности))

Направленность (профиль) подготовки
Оптические системы и сети связи
(указывается наименование направленности (профиля) подготовки)

Квалификация
Бакалавр
(указывается квалификация)

Разработчик (составитель)
к.ф.-м.н.,
(должность, ученая степень, ученое звание)

 /Сагитов Р.Г...

Для приема 2021 г.
Уфа - 2021г.

Составитель / составители:, к.ф.-м.н., Сагитов Р.Г.

Рабочая программа дисциплины утверждена на заседании кафедры инфокоммуникационных технологий и наноэлектроники протокол №5 от 17.02.2021

Заведующий кафедрой  Салихов Р.Б.

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	
2. Цель и место дисциплины в структуре образовательной программы	
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	
4. Фонд оценочных средств по дисциплине	
4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах информирования, описание шкал оценивания	
4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций	
4.3. Рейтинг-план дисциплины (при необходимости)	
5. Учебно-методическое и информационное обеспечение дисциплины	
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины	
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

(с ориентацией на карты компетенций)

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
	ПК-7 - Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	ПК 7.1. Знать способы осуществления администрирования средствобеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов ПК-7.2. Уметьосуществлять администрирование средствобеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) ПК-7.3.Владеть способностью администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Знать способы осуществления администрирования средствобеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов Уметь осуществлять администрирование средствобеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) Владеть способностью администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности сетей и систем связи» относится части, формируемая участниками образовательных отношений образовательной программы (дисциплина по выбору).

Дисциплина изучается на 4 курсе в 7 семестре.

Цели и место изучения дисциплины: является изучение основ информационной безопасности и защиты информации в системах и сетях связи при их создании и эксплуатации. Дисциплина «Основы информационной безопасности сетей и систем связи» относится к вариативной части образовательной программы (дисциплина по выбору).

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:

1. Правоведение
2. Вычислительная техника и информационные технологии
3. Сети связи и системы коммутации

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ПК 7.Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Зачет

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	**Критерии оценивания результатов обучения**	
		«Не зачтено»	«Зачтено»
ПК 7.1. Знать способы администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Знать способы администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Отсутствие знаний или только фрагментарные представления о способахадминистрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Достаточно хорошо (возможнонеполные) изложены знания о способахадминистрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколовосуществления развития транспортных сетей и сетей передачиданных, включая сети радиодоступа, спутниковых систем, коммутационных подсистем и сетевыхплатформ)
ПК-7.2. Уметь осуществлять администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Уметьосуществлять администрирование средств обеспечения безопасности удаленного доступа (операционных системи специализированныхпротоколов)	Отсутствие умений или только фрагментарные умениеосуществлять администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	В целом успешное (возможно и не систематическое) умение осуществлять администрирование средств обеспечения безопасности удаленного доступа (операционныхсистем и специализированных протоколов)
ПК-7.3. Владеть способностью администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Владеть способностью администрирования средств обеспечения безопасности удаленного доступа (операционных системи специализированных протоколов)	Отсутствие владениеспособностью осуществления администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	В целом успешное владение способностью осуществления администрирования средств обеспечения безопасности удаленногодоступа (операционных систем и специализированных протоколов)

Показатели сформированности компетенции:

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов).

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК 7.1. Знать способы осуществления администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) ПК-7.2. Уметь осуществлять администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) ПК-7.3. Владеть способностью администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Знать способы осуществления администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	контрольная работа; тесты; защита отчетов по лабораторным работам; зачет
	Уметь осуществлять администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	
	Владеть способностью администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	

…Вопросы к зачету:

1. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
2. Покажите связь между уровнем развития общества и технологиями защиты информации.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. С чем связан возросший интерес к проблемам защиты информации?
6. Каковы отличия формального и неформального подходов к проблемам защиты информации?
7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?

8. Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
9. Каковы правовые понятия в области защиты информации?
10. Что такое защита информации? Информационная безопасность?
11. Охарактеризуйте понятия, связанные с организацией защиты информации. 12. Каковы основные принципы построения систем защиты информации?
13. Что такое комплексный подход к обеспечению информационной безопасности?

Примеры тестовых заданий (для рубежного контроля)

1. Как называется умышленно искаженная информация?
   а) Дезинформация
   б) Информативный поток
   в) Достоверная информация
   г) Перестает быть информацией

2. Как называется информация, к которой ограничен доступ?
   а) Конфиденциальная
   б) Противозаконная
   в) Открытая
   г) Недоступная
3. Какими путями может быть получена информация?
   а) проведением, покупкой и противоправным добыванием информации научных исследований
   б) захватом и взломом ПК информации научных исследований
   в) добыванием информации из внешних источников и скремблированием информации научных исследовании
   г) захватом и взломом защитной системы для информации научных исследований

4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
   а) защищенные КС
   б) небезопасные КС
   в) самодостаточные КС
   г) саморегулирующиеся КС

5. Основной документ, на основе которого проводится политика информационной безопасности?
   а) программа информационной безопасности
   б) регламент информационной безопасности
   в) политическая информационная безопасность
   г) протекторат

6) В зависимости от формы представления информация может быть разделена на… а) речевую, документированную и телекоммуникационную
   б) мысль, слово и речь
   г) цифровая, звуковая и тайная
   в) цифровая, звуковая

Критерии оценки (в баллах):
За каждый правильный ответ- 1 балл
За ошибочный ответ – 0 баллов

Лабораторные работы

Порядок выполнения лабораторных работ приведен в «Описании лабораторных работ по дисциплине «Основы информационной безопасности сетей и систем связи», имеющихся в специализированной лаборатории (ауд. 210 физ.-мат. корп. БашГУ).

Тематика и перечень лабораторных работ:

1. Моделирование IPSec VPN в Cisco Packet Tracer
2. Настройка Firewall на маршрутизаторе в Cisco Packet Tracer
3. Работа протокола Radius в Cisco Packet Tracer
4. Шифрование с открытым ключом и электронная цифровая подпись на GPG
5. Метод шифрования с открытым ключом RSA
6. Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.

Критерии оценки (в баллах)

Работа выполнена, к отчету нет существенных замечаний 5 баллов Работа выполнена, отчет не представлен или в нем имеются существенные 2 баллов недостатки

Работа не выполнена 0 баллов

Примеры вопросов для устного опроса и для проведения зачета (для заочной формы обучения)

1. Назовите известные вам модели защиты от несанкционированного доступа к информации.
2. Перечислите основные принципы защиты информации от несанкционированного доступа. В чем суть каждого из них?
3. В чем отличие идентификации от аутентификации пользователей?
4. Раскройте основные особенности известных методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
5. Какие основные способы шифрования вы знаете? Каковы их приемущества и недостатки?

Развернутость и полнота ответов на вопросы определяется в соответствии с критериями из п.4.1
За правильный развернутый полный ответ - 10
баллов За правильный, но неполный ответ – 5
баллов
За ошибочный ответ или отсутствие ответа – 0 баллов

Критерии оценивания для заочной формы обучения:

Обучающиеся заочной формы обучения допускаются к сдаче зачета при условии выполнения всех предложенных лабораторных работ и тестирования, в результате которого будет дано не менее 50% правильных ответов.

- оценка «зачтено» выставляется студенту, если он ответил на 2 вопроса из перечня;
- оценка «не зачтено» выставляется студенту, если он не ответил на один или оба

вопроса.

Ответы на вопросы должны соответствовать критериям оценивания результатов обучения, приведенным в разделе 4.1.

Участие в конференциях, публикация статей

1. Публикация статей – *5 баллов*

Критерии	Оценка (в баллах)	
Тип работы	Реферативная работа	0,1
	Работа носит исследовательский характер	0,3
	Работа является исследованием	0,6
Использование известных данных и научных фактов	Не использует никаких данных	0
	Автор использовал известные данные	0,4
	Использованы уникальные научные данные	0,6
Полнота цитируемой литературы, ссылка на	Использован учебный материал	0,1
	Использованы специализированные издания	0,3
ученых	Использованы интернет ресурсы	0,6
Актуальность работы	Изучение вопроса не является актуальным	0
	Представленная работа привлекает интерес своей актуальностью	0,4
	Работа содержит научный характер	0,6
Степень новизны полученных результатов	Работа не содержит ничего нового	0
	В работе доказан уже установленный факт	0,4
	В работе получены новые данные	0,6

2. Участие в конференции- *5 баллов*

Творческий подход к отбору и структурированию материала - *1 балл*
Новизна и самостоятельность при постановке проблемы - *1 балл*
Выступление не является простым чтением с экрана - *1 балл*
В выступлении дополняются и раскрываются ключевые моменты, представленные на слайдах - *1 балл*
Во время выступления поддерживается зрительный контакт с аудиторией, речь отличается богатством интонаций - *1 балл*

4.3. Рейтинг-план дисциплины (при необходимости)

Рейтинг–план дисциплины

Основы информационной безопасности сетей и систем связи

специальность Инфокоммуникационные технологии и системы связи курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль I Информационное общество и информационная безопасность.				
Текущий контроль				
1. Устный опрос	10	2	0	20
Рубежный контроль				
1. Письменное тестирование	25	1	0	25
Модуль II Технические аспекты информационной безопасности				
Текущий контроль				
1. Выполнение лабораторных работ	2	6	0	12
2. Выполнение расчетов, оформление и защита отчетов по лабораторным работам	3	6	0	18
Рубежный контроль				
1. Письменное тестирование	25	1	0	25
Поощрительные баллы				
1. Участие в студенческих научных конференциях, выставках, конкурсах.	10	1	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Непосещение лекционных занятий			0	-6
2. Непосещение практических занятий			0	-10
Итоговый контроль				
1. Зачет	0	1	0	0

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для

освоения дисциплины

Основная литература:

1. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170 (19.02.2018).
2. Технические средства и методы защиты информации : учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. ; под ред. А.П. Зайцева, А.А. Шелупанова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком, 2012. - 616 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0084-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253207 (19.02.2018).
3. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам

/ Г.А. Бузов. - Москва : Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0424-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457143 (19.02.2018).

Дополнительная литература:

1. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - Москва : Горячая линия - Телеком, 2011. - 558 с. : ил. - ISBN 5-93517-292-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253056 (19.02.2018).
2. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации): юридическая ответственность за правонарушения : учебное пособие / В.К. Новиков. - Москва : Горячая линия-Телеком, 2015. - 175 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0525-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457171 (19.02.2018).
3. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, К.В. Славнов, Е.В. Кравцов ; под ред. А.В. Душкина. - Москва : Горячая линия - Телеком, 2016. - 248 с. : схем., табл., ил. - Библиогр.: с. 234-235 - ISBN 978-5-9912-0470-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=483768 (19.02.2018).
4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др. ; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стер. - Москва : Горячая линия - Телеком, 2012. - 552 с. : ил. - Библиогр.: с. 244-246 - ISBN 978-5-9912-0257-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=252979 (19.02.2018)

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1	Электронно-библиотечная система «ЭБ БашГУ»	Собственная электронная библиотека учебных и научных	Авторизованный доступ по паролю из любой точки	Регистрация в Библиотеке БашГУ,	https://elib.bashedu.ru/

		электронных изданий, которая включает издания преподавателей БашГУ	сети Интернет	дальнейший доступ из любой точки сети Интернет	
2	Электронно-библиотечная система «Университетская библиотека online»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://www.biblioclub.ru/
3	Электронно-библиотечная система издательства «Лань»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://e.lanbook.com/

6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование дисциплины (модуля), практик в соответствии с учебным планом	Наименование специальных помещений и помещений для самостоятельнойработы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
Основы информационной безопасности сетей и систем связи	**1.Учебные аудитории для проведения учебных занятий:** Аудитория № 415 Аудитория №414 Лаборатория сетей связи и систем коммутации **2.Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду организации:** Читальный зал №2	**Аудитория №415** Оборудование: доска, учебная мебель, проектор **Аудитория №414 Лаборатория сетей связи и систем коммутации** Оборудование: учебная мебель, доска аудиторная, моноблок ThinkCentre (12 шт.); проектор мультимедийный, экран; макет ЦСК «Элком», макет ЦСП Морион ИКМ – 30; ЦАТС-М200 – 1 шт.; источник электропитания УЭПС-2 **Читальный зал № 2** Оборудование: учебный и научный фонд, научная периодика, неограниченный доступ к ЭБС и БД; ПК (моноблок) - 8 шт.; количество посадочных мест - 80	**Лицензионное программное обеспечение:** 1. Windows 8 Russian; Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензия- OLP NL Academic Edition. Бессрочная. 2. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензия-OLP NL Academic Edition. Бессрочная. 3.OrCAD 16.6 Lite (лицензия GNU GPL, свободное программное обеспечение). 4.MikroC PRO for PIC (лицензия GNU GPL, свободное программное обеспечение). 5.Лицензия Circuit Design Suite исх. № и-1614/20 от 19.11.2020, срок лицензии-бессрочно. 6.Лицензия LabVIEW FDS исх. № и-1613/20 от 19.11.2020, срок лицензии-бессрочно. **Лицензионное программное обеспечение, позволяющее проводить компьютерное тестирование:** Moodle «Официальный оригинальный английский текст лицензии для системы Moodle - <http://www.gnu.org/licenses/gpl.html> Перевод лицензии для системы Moodle - http://rusgpl.ru/rusgpl.pdf»

Приложение № 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Основы информационной безопасности сетей и систем связи
на 7 семестр

очная
форма обучения

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3/108
Учебных часов на контактную работу с преподавателем:	
лекций	18
практических/ семинарских	-
лабораторных	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	53,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	-

Форма(ы) контроля:
зачет *7* семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СРС			
1	2	4	5	6	7	8	9	10
1.	Радиочастотный ресурс, его использование и распределение.Основы излучения и приема электромагнитных волн. Типы и характеристики антенн.Чувствительность приемников систем подвижной связи.Энергетика приема и передачи электромагнитных волн. Модель свободного пространства.Модели распространения электромагнитных волн.	4	-	36	18	[1]:гл.3,7 [3]:гл. 5 [4]	[1]:гл.3,7 [3]:гл. 5 [4]	Лабораторные работы ; тест
2.	Энергетический баланс системы подвижной связи. Методы доступа к среде и дуплексирования.Коэффициент повторного использования частот. Типы кластеров.	2	-	-	12	[1]:гл.5 [2]:гл.11 [3]:гл.2,9 [4]	[1]:гл.5 [2]:гл.11 [3]:гл.2,9 [4]	тест
3.	Профессиональные системы подвижной связи. Системы беспроводной телефонии. Сотовые системы подвижной связи. История и классификация. Сравнение емкости различных систем сотовой связи. Сотовая система подвижной связи CDMAOne.	2	-	-	8	[2]:гл.12 [4]	[3]:гл. 6-9 [4]	тест

4.	Сотовая система подвижной связи GSM. Общее описание системы. Устройство мобильного терминала GSM.Формирование кадров, обработка речи в GSM. Типы физических и логических каналов GSM. Модуляция сигнала в GSM Роуминг в GSM. Процедуры при международном вызове.Обеспечение безопасности в GSM. SIM-карта.Способы уменьшения интерференции и повышения емкости в GSM	4	-	-	8	[2]:гл.12 [3]:гл.6,10 [4]	[3]:гл.6,10 [4]	тест
5	Решения для систем поколения 2.5. GPRS, EDGE. Системы мобильной связи 3 поколения, HSDPA. Системы мобильной связи 4 поколения, LTE и его особенности.	6	-	-	7,8	[2]:гл.12.6 [3]:гл.7,17 [4]	[2]:гл.12.6 [3]:гл.7,17 [4]	тест
	Всего часов:	18	-	36	53,8			