Аннотация к рабочей программе дисциплины «Защита информации в системах беспроводной связи»

Цель преподавания дисциплины

Дисциплина «Защита информации в системах беспроводной связи» является получение студентами знаний о принципах и методах защиты систем беспроводной связи, навыков по защите абонентских терминалов.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

1) получить знания о методах подавления радиосигнала путем его зашумления;

– получить знания о методах защиты радиоэлектронных средств (РЭС) передачи речевых сигналов от средств радиоэлектронного подавления (РЭП) при воздействии широкополосных аддитивных помех;

2) получить знания о методах защиты абонентского терминала в системе сотовой связи GSM;

3) получить знания о методах защиты терминала беспроводной связи Bluetooth в системе Android;

4) получить знания о методах радиоподавления средств радиосвязи и принципах расчета эффективности радиоподавления;

5) получить знания о методах защиты средств радиосвязи от нарушения конфиденциальности путем использования скремблирования и шифрования;

6) получить знания о методах защиты информации в системах беспроводной связи путем имитозащиты передаваемых сообщений;

7) получить знания о методах сигнальной помехозащиты радиолиний в системах беспроводной связи;

8) ознакомление с методами оценки помехозащиты спутниковой линии связи;

9) ознакомление с методами повышения скрытности РЭС и оценки их эффективности.

Компетенции, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6);

– способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13);

– способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14).

Разделы дисциплины

Краткий обзор систем беспроводной связи. Основы радиоэлектронной бизнесс-разведки. Радиоэлектронное подавление. Последовательность расчета R_n . Нарушения нормального функционирования средств беспроводной связи. Помехозащита радиолиний. Безопасность спутниковой связи. Спутниковые технологии VSAT и информационная безопасность сети. Информационная безопасность сотовой связи GSM. Обеспечение секретности абонента. Инфобезопасность транкинговых систем связи. Основы радиоэлектронной борьбы и радиоэлектронного подавления. Радиоэлектронное подавление. Последовательность расчета R_n . Нарушения нормального функционирования средств беспроводной связи. Помехозащита радиолиний. Безопасность спутниковой связи. Спутниковые технологии VSAT и информационная безопасность сети. Информационная безопасность сотовой связи GSM. Обеспечение секретности абонента. Инфобезопасность транкинговых систем связи.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
информатики
(наименование факультета полностью)
_____ Т.А. Ширабакина
(подпись, инициалы, фамилия)
«_1_» _____02_____ 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

(наименование дисциплины)

направления подготовки (специальность) 10.05.02

(шифр согласно ФГОС

«Информационная безопасность телекоммуникационных систем»

и наименование направления подготовки (специальности)

«Защита информации в системах связи и управления»

наименование профиля, специализации или магистерской программы

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2017

2

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем и на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Учёным советом университета, протокол №5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.05.02 Информационная безопасность телекоммуникационных систем на заседании кафедры информационной безопасности №8 «1» 02 2017 г.

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы Лысенко В.Л.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол №5 «30» 01 2017г. на заседании кафедры информационной безопасности 28.08.2017, №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности 23.06.2018, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019, №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №7 «30» 01 2017 г. на заседании кафедры информационной безопасности протокол №1 от 31.08.2020 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности протокол №11 от 28.06.2021 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности протокол №11 от 30.06.22 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности протокол №11 от 30.06.2023

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

---

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина «Защита информации в системах беспроводной связи» является получение студентами знаний о принципах и методах защиты систем беспроводной связи, навыков по защите абонентских терминалов.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

−получить знания о методах подавления радиосигнала путем его зашумления;

– получить знания о методах защиты радиоэлектронных средств (РЭС) передачи речевых сигналов от средств радиоэлектронного подавления (РЭП) при воздействии широкополосных аддитивных помех;

– получить знания о методах защиты абонентского терминала в системе сотовой связи GSM;

– получить знания о методах защиты терминала беспроводной связи Bluetooth в системе Android;

– получить знания о методах радиоподавления средств радиосвязи и принципах расчета эффективности радиоподавления;

– получить знания о методах защиты средств радиосвязи от нарушения конфиденциальности путем использования скремблирования и шифрования;

−получить знания о методах защиты информации в системах беспроводной связи путем имитозащиты передаваемых сообщений;

−получить знания о методах сигнальной помехозащиты радиолиний в системах беспроводной связи;

−ознакомление с методами оценки помехозащиты спутниковой линии связи;

– ознакомление с методами повышения скрытности РЭС и оценки их эффективности.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

– общие характеристики систем беспроводной электросвязи;

– основные аспекты инфокоммуникационной безопасности систем беспроводной связи;

– основные угрозы аспектам инфокоммуникационной безопасности систем беспроводной связи;

уметь:

– оценивать помехозащиту систем беспроводной связи;

– классифицировать помехи и их влияние на работу радиоэлектронных средств;

владеть:

– методами защиты беспроводных систем связи;

– методами повышения скрытности РЭС и оценки их эффективности.

Процесс изучения дисциплины направлен на формирование следующих компетенций*:*

– способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6);

– способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13);

– способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к базовой части теоретического курса (Б1.Б.39). Изучается на 5 курсе в 9 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 академических часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72,1
лекции	36
лабораторные занятия	18
практические занятия	18
экзамен	0
зачет	0,1
курсовая работа (проект)	Не

	предусмотрена
расчетно-графическая (контрольная) работа	Не предусмотрена
Аудиторная работа (всего):	72
в том числе:	
лекции	36
лабораторные занятия	18
практические занятия	18
Самостоятельная работа обучающихся (всего)	36
Контроль/экз (подготовка к экзамену)	0

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Краткий обзор систем беспроводной связи	Общая характеристика систем электросвязи: системы проводной и беспроводной связи. Принципиальное отличие радиосистем передачи информации от проводных систем. Диапазоны частот радиосистем. Симплексная, полудуплексная и дуплексная радиосвязь. Классификация систем беспроводной связи. Системы узкополосной радиосвязи: радионаправление и радиосеть, системы прямой радиосвязи и системы с переотражением. Системы широкополосной радиосвязи: системы прямой радиосвязи и радиорелейные системы. Основные аспекты инфокоммуникационной безопасности СБС: доступность, целостность и конфиденциальность. Основные угрозы аспектам инфокоммуникационной безопасности СБС.
2.	Основы радиоэлектронной бизнесс-разведки	Основы радиоэлектронной бизнес-разведки. Демаскирующие признаки объектов и действий. Назначение, задачи и особенности радиоэлектронной бизнес-разведки. Характеристика видов радиоэлектронной бизнес-разведки. Радиоразведка и радиотехническая разведка. Помехи, классификация помех и их влияние на

		функционирование радиоэлектронных средств.
3.	Основы радиоэлектронной борьбы и радиоэлектронного подавления	Радиоэлектронная борьба и радиоэлектронное подавление. Пассивные и активные целенаправленные радиопомехи, выбор структуры радиопомех, маскирующие и имитирующие радиопомехи.
4.	Радиоэлектронное подавление	Радиоподавление, зффективность радиоэлектронного подавления, условия эффективного радиоподавления, показатели и критерии его эффективности.
5.	Последовательность расчета R_n	Радиоподавление, зффективность радиоэлектронного подавления, условия эффективного радиоподавления, показатели и критерии его эффективности.
6.	Нарушения нормального функционирования средств беспроводной связи	Общие методы и средства защиты беспроводных систем связи от радиоэлектронного подавления, четыре основных требования к защищенности беспроводной системы связи. Методы защиты радиосистем от средств бизнес-разведки: крипто- и имитозащита сообщений.
7.	Помехозащита радиолиний	Методы сигнальной помехозащиты: уравнение помехозащиты, применение методов фильтрации и программной перестройки частоты, функциональная схема помехозащищенной радиолинии.
8.	Безопасность спутниковой связи	Безопасность спутниковой связи: общая характеристика систем спутниковой связи, основные угрозы безопасности, методы и средства защиты.
9.	Спутниковые технологии VSAT и информационная безопасность сети	Информационная безопасность радиорелейной связи: общая характеристика систем радиорелейной связи, основные угрозы безопасности, методы и средства защиты.
10.	Информационная безопасность сотовой связи GSM	Информационная безопасность узкополосных систем сотовой связи: общая характеристика систем сотовой связи, основные угрозы безопасности, методы и средства защиты.
11.	Обеспечение секретности абонента	Обеспечение секретности абонента. Угрозы информационной безопасности при использовании сотовых систем связи. Нарушение связи в сотовых сетях. Нарушение конфиденциальности информации, передаваемой в сотовых сетях связи. Клонирование SIM-карты.
12.	Инфобезопасность	Информационная безопасность узкополосных

	транкинговых систем связи	систем транкинговой связи: общая характеристика систем транкинговой связи, основные угрозы безопасности, методы и средства защиты.
13.	Стандарт TETRA	Распределение сеансовых ключей аутентификации по базовым станциям. Алгоритм аутентификации пользователей с применением сеансовых ключей. Возможности по разграничению доступа к передаваемой информации. Четыре алгоритма шифрования (TEA1 – TEA4). Поточный метод шифрования.
14.	Безопасность широкополосных систем радиосвязи	Информационная безопасность широкополосных систем радиосвязи: общая характеристика систем широкополосной радиосвязи, основные угрозы безопасности, методы и средства защиты.
15.	Виды удаленных атак на устройства с поддержкой Bluetooth	Классификация видов удаленных атак. Атака типа bluesnarfing. Защита от атак на широкополосную систему беспроводной передачи данных.
16.	Защита сетей Wi-Fi	Особенности беспроводной связи с точки зрения безопасности. Риски безопасности. Легкость в развертывании и мобильность. Особенности атаки.
17.	Обеспечение безопасного функционирования беспроводных сетей. Риски.	Четыре риска безопасности. Разведка. Имперсонация и Identity Theft.
18.	Отказы в обслуживании.	Специализированные инструменты атакующего. Denial of Service, DoS. Активность в нерабочее время. Скорости. Интерференция. Связь.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			

1	2	3	4	5	6	7	8
1.	Краткий обзор систем беспроводной связи	2	-	-	О – 1 Д – 1, 4	С2	ПК-6
2.	Основы радиоэлектронной бизнесс-разведки	2	1	-	О – 1 Д – 1, 4 МУ – 1	С2, КО2	ПК-6
3.	Основы радиоэлектронной борьбы и радиоэлектронного подавления	2	2	-	О – 1 Д – 1, 4 МУ – 2	С3, КО3	ПК-13
4.	Радиоэлектронное подавление	2	-	1	О – 1 Д – 5 МУ – 6	С4, КО4	ПК-13
5.	Последовательность расчета R_n	2	-	2	О – 1 Д – 6 МУ – 7	С5, КО5	ПК-14
6.	Нарушения нормального функционирования средств беспроводной связи	2	-	3	О – 1 Д – 2, 3 МУ – 8	С6, КО6	ПК-13
7.	Помехозащита радиолиний	2	-	4	О – 1 Д – 2, 3 МУ – 9	С7, КО7	ПК-14
8.	Безопасность спутниковой связи	2	-	5	О – 1 Д – 3, 6 МУ – 10	С8, КО8	ПК-6
9.	Спутниковые технологии VSAT и информационная безопасность сети	2	-	6	О – 2 Д – 7 МУ – 11	С9, КО9	ПК-6
10.	Информационная безопасность сотовой связи GSM	2	3	-	О – 2 Д – 6 МУ – 3	С10, КО10	ПК-6
11.	Обеспечение секретности абонента	2	4	-	О – 2 Д – 5 МУ – 4	С11, КО11	ПК-14
12.	Инфобезопасность транкинговых систем связи	2	-	-	О – 2 Д – 5, 7	С12	ПК-14

1	2	3	4	5	6	7	8
13.	Стандарт TETRA	2	-	-	О – 1 Д – 3, 6	С13	ПК-14
14.	Безопасность широкополосных систем радиосвязи	2	-	-	О – 1 Д – 1, 2	С14	ПК-13
15.	Виды удаленных атак на устройства с поддержкой Bluetooth	2	5	-	О – 1 Д – 6 МУ – 5	С15, КО15	ПК-6
16.	Защита сетей Wi-Fi	2	-	-	О – 2 Д – 4	С16	ПК-14
17.	Обеспечение безопасного функционирования беспроводных сетей. Риски	2	-	-	О – 2 Д – 4,7	С17	ПК-6
18.	Отказы в обслуживании	2	-	-	О – 2 Д – 3, 5	С18	ПК-6

С – собеседование, КО – контрольный опрос

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные работы

Таблица 4.3 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Лабораторная работа №1 «Подавление радиосигнала радиопомехой»	5
2.	Лабораторная работа №2 «Исследование метода защиты речевых сигналов от воздействия широкополосных аддитивных помех»	5
3.	Лабораторная работа №3 «Исследование методов защиты абонентского терминала в системе сотовой связи GSM»	3
4.	Лабораторная работа №4 «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»	2
5.	Лабораторная работа №5 «Исследование методов защиты терминала беспроводной связи Bluetooth»	3
Итого		18

4.2.2. Практические занятия

Таблица 4.4 – Практические занятия

№	Наименование практического занятия	Объем, час.
1.	Выполнение практического задания №1 «Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления»	3
2.	Выполнение практического задания №2 «Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности»	3
3.	Выполнение практического задания №3 «Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений»	3
4.	Выполнение практического задания №4 «Методы сигнальной помехозащиты радиолиний»	3
5.	Выполнение практического задания №5 «Оценка помехозащиты спутниковой линии связи»	3
6.	Выполнение практического задания №6 «Оценка эффективности применения методов повышения скрытности РЭС»	3
Итого		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Краткий обзор систем беспроводной связи	1 неделя	4
2.	Основы радиоэлектронной бизнесс-разведки	2 неделя	4
3.	Основы радиоэлектронной борьбы и радиоэлектронного подавления	3 неделя	4
4.	Радиоэлектронное подавление	4 неделя	4
5.	Последовательность расчета R_n	5 неделя	4
6.	Нарушения нормального функционирования средств беспроводной связи	6 неделя	4
7.	Помехозащита радиолиний	7 неделя	4
8.	Безопасность спутниковой связи	8 неделя	4
9.	Спутниковые технологии VSAT и	9 неделя	4

	информационная безопасность сети		
10.	Информационная безопасность сотовой связи GSM	10 неделя	4
11.	Обеспечение секретности абонента	11 неделя	4
12.	Инфобезопасность транкинговых систем связи	12 неделя	4
13.	Стандарт TETRA	13 неделя	4
14.	Безопасность широкополосных систем радиосвязи	14 неделя	4
15.	Виды удаленных атак на устройства с поддержкой Bluetooth	15 неделя	4
16.	Защита сетей Wi-Fi	16 неделя	4
17.	Обеспечение безопасного функционирования беспроводных сетей. Риски	17 неделя	4
18.	Отказы в обслуживании	18 неделя	4
Итого			72

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем составления заданий для самостоятельной работы;

– путем разработки вопросов к зачету, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение практикоориентированных заданий в ходе лабораторных занятий.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Лабораторная работа №1 «Подавление радиосигнала радиопомехой»	Работа в программе Adobe Audition.	2
2.	Лабораторная работа №2 «Исследование метода защиты речевых сигналов от воздействия широкополосных аддитивных помех»	Работа в программе Adobe Audition.	2
3.	Лабораторная работа №3 «Исследование методов защиты абонентского терминала в системе сотовой связи GSM»	Исследование функционала ОС Android.	2
4.	Лабораторная работа №4 «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»	Исследование функционала ОС Android.	2
5.	Лабораторная работа №5	Исследование	2

	«Исследование методов защиты терминала беспроводной связи Bluetooth»	функционала ОС Android.	
6.	Выполнение практического задания №2 «Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности»	Выполнение студентом интерактивных заданий по освоению методов защиты информации в СБС.	2
	Итого		12

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного

потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная		
	начальный	основной	завершающий
1	2	3	4
применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6)	Защита информации в системах беспроводной связи**	Комплексное обеспечение информационной безопасности инфокоммуникационных систем**	Конструкторская практика Государственная итоговая аттестация
организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13)	Системы коммутации** Защита информации в системах беспроводной связи**	Основы мониторинга безопасности инфокоммуникационных систем и сетей**	Практика по получению профессиональных умений и опыта профессиональной деятельности
выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и	Антенны и распространение радиоволн	Техническая защита информации**	Антенны и распространение радиоволн Информационная безопасность телекоммуникационных систем Аппаратные средства телекоммуникацио

систем (ПК-14)			нных систем Программно-аппаратные средства обеспечения информационной безопасности Защита информации в системах беспроводной связи Защита информации в компьютерных сетях Электропитание устройств и систем телекоммуникаций Безопасность операционных систем и баз данных Безопасность систем и сетей передачи данных Средства мониторинга систем и сетей передачи сообщений Методы и средства радиомониторинга Практика по получению профессиональных умений и опыта профессиональной деятельности Эксплуатационная практика

**Этапы для РПД всех форм обучения определяются по учебному плану очной формы обучения следующим образом:*

Этап	Учебный план очной формы обучения/ семестр изучения дисциплины		
	Бакалавриат	Специалитет	Магистратура
Начальный	1-3 семестры	1-3 семестры	1 семестр
Основной	4-6 семестры	4-6 семестры	2 семестр
Завершающий	7-8 семестры	7-10 семестры	3-4 семестр

** Если при заполнении таблицы обнаруживается, что *один или два этапа* не обеспечены дисциплинами, практиками, НИР, необходимо:

- при наличии дисциплин, изучающихся в разных семестрах, – распределить их по этапам в зависимости от № семестра изучения (начальный этап соответствует более раннему семестру, основной и завершающий – более поздним семестрам);
- при наличии дисциплин, изучающихсяв одном семестре, – все дисциплины указать для всех этапов.

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Наименование компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и	**Знать**: основное понятие ИБ ТКС, основные её функции **Уметь**: анализировать научно-техническую информацию ИБ СБС. **Владеть навыками**: оценки различных компонентов подсистем обеспечения ИБ СБС.	**Знать**: принципы организации подситем безопасности СБС. **Уметь**: анализировать научно-техническую информацию и нормативные материалы ИБ СБС. **Владеть навыками**: составления аналитического отчета о состоянии ИБ СБС.	**Знать**: критерии соответствия функционала подсистем информационной безопасности СБС угрозам для объектов информатизации. **Уметь**: анализировать научно-техническую информацию и нормативные и методические материалы ИБ СБС. **Владеть навыками**: составления методических комплексов по

среду (ПК-6)	нестандартных ситуациях			ИБ СБС.
организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: основное понятие ИБ СБС, основные её функции **Уметь**: организовывать выполнение режима защиты информации **Владеть навыками**: ограничения доступа к информации.	**Знать**: принципы составления регламентирующих документов **Уметь**: настраивать программно-аппаратные системы защиты информации СБС. **Владеть навыками**: администрирования программно-аппаратных СЗИ СБС.	**Знать**: критерии соответствия функционала подсистем информационной безопасности СБС угрозам для объектов информатизации. **Уметь**: разрабатывать проекты документов, регламентирующих работу по обеспечению ИБ СБС. **Владеть навыками**: организации выполнения требований режима защиты информации ограниченного доступа.
способность выполнять установку, настройку,	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН,	**Знать**: понятие подсистему управления ИБ, основные её функции **Уметь**: выполнять	**Знать**: принципы организации подситем безопасности предприятий **Уметь**: настраивать	**Знать**: критерии соответствия функционала подсистем информационной безопасности угрозам для объектов

обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14)	установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	сервисные мероприятия с системами программно-аппаратной защиты информации **Владеть навыками**: эксплуатации различных компонентов подсистем обеспечения ИБ	программно-аппаратные системы защиты информации **Владеть навыками**: администрирования программно-аппаратных СЗИ	информатизации **Уметь**: выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление телекоммуникационного оборудования **Владеть навыками**: реагировании на нештатные ситуации, возникающие при эксплуатации программно-аппаратных СЗИ

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

	Раздел	Код контроли-	Технология	Оценочные	Описание

п/п	(тема) дисциплины	руемой компе-тенции (или её части)	формирова-ния	наимено вание	№№ заданий	шкал оценивания
1	2	3	4	5	6	7
1.	Краткий обзор систем беспроводной связи	ПК-6	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
2.	Основы радиоэлектронной бизнесс-разведки	ПК-6	Лекция, СРС, лабораторная работа	Собеседование	1-6	Согласно табл.7.2
				Контроль ные вопросы к ЛР№1	1-4	
3.	Основы радиоэлектронной борьбы и радиоэлектронного	ПК-13	Лекция, СРС, лабораторная работа	Собеседование	1-6	Согласно табл.7.2
				Контроль ные вопросы к ЛР№2	1-8	
4.	Радиоэлектронное подавление	ПК-13	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контроль ные вопросы к ПР№1	1-12	
5.	Последовательность расчета R_n	ПК-14	Лекция, СРС, практическое занятие	Собеседование	1-4	Согласно табл.7.2
				Контроль ные вопросы к ПР№2	1-11	
6.	Нарушения нормального	ПК-13	Лекция, СРС, практическ	Собеседование	1-6	Согласно табл.7.2

	функционирования средств беспроводной связи		ое занятие	Контрольные вопросы к ПР№3	1-7	
7.	Помехозащита радиолиний	ПК-14	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ПР№4	1-7	
8.	Безопасность спутниковой связи	ПК-6	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ПР№5	1-6	
9.	Спутниковые технологии VSAT и информационная безопасность сети	ПК-6	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ПР№6	1-12	
10.	Информационная безопасность сотовой связи GSM	ПК-6	Лекция, СРС, лабораторная работа	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ЛР№3	1-6	

11.	Обеспечение секретности абонента	ПК-14	Лекция, СРС, лабораторная работа	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ЛР№4	1-6	
12.	Инфобезопасность транкингов	ПК-14	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
13.	Стандарт TETRA	ПК-14	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
14.	Безопасность широкополосных систем	ПК-13	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
15.	Виды удаленных атак на устройства с поддержкой Bluetooth	ПК-6	Лекция, СРС, лабораторная работа	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ЛР№5	1-5	
16.	Защита сетей Wi-Fi	ПК-14	Лекция, СРС	Собеседование	1-2	Согласно табл.7.2
17.	Обеспечение безопасного функционирования	ПК-6	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
18.	Отказы в обслуживании	ПК-6	Лекция, СРС	Собеседование	1-3	Согласно табл.7.2

Примеры типовых контрольных заданий для текущего контроля

Вопросы собеседования по разделу (теме) 1. «Краткий обзор систем беспроводной связи».

1. Что такое системы электросвязи, и на какие виды они делятся в зависимости от среды распространения?
2. Какую полосу частот занимают диапазоны частот радиосистем?

3. Какие бывают виды радиосвязи?
4. Перечислите основные факторы, оказывающие влияние на величину напряженности поля в точке приема.
5. На какие системы делятся СБС по типу используемой технологии?
6. Что такое радиосеть?

Контрольные вопросы к практической работе по теме «Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления»

1. Что такое РЭП?
2. Основная цель РЭП и решаемые ею задачи?
3. Какие аспекты инфокоммуникационной безопасности СБС нарушает РЭП?
4. Что такое эффективность РЭП, какие известны виды реализуемого ущерба?
5. Основной показатель для оценки эффективности РЭП, как он определяется?
6. Какие условия необходимо выполнить для эффективного подавления СБС?
7. Основной критерий для оценки эффективности РЭП, как он определяется?
8. Что такое коэффициент подавления и от каких факторов он зависит?
9. Из каких этапов состоит процесс решения прямой задачи РЭП?
10. Что такое электромагнитная доступность СБС?
11. Какие факторы влияют на предельную дистанцию Rп РЭП УКВ радиосвязи?
12. Какие факторы влияют на величину коэффициента подавления Квх на входе приемного устройства подавляемого канала связи? Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Контрольные вопросы к лабораторной работе по теме «Подавление радиосигнала радиопомехой»

1. Классификация систем беспроводной связи.
2. Что такое радиоподавление.
3. Перечислить особенности метода радиоподавления сигнала помехой.
4. Объяснить порядок определения текущего коэффициента подавления.

Типовые задания для промежуточной аттестации.

Промежуточная аттестация по дисциплине проводится в форме

зачета. Зачет проводится в форме тестирования (бланкового и/или компьютерного).

Для тестирования используются контрольно-измерительные материалы (КИМ)

– задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Лабораторная работа №1 «Подавление радиосигнала радиопомехой»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №2 «Исследование метода защиты речевых сигналов от воздействия широкополосных аддитивных помех»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №3 «Исследование методов защиты абонентского терминала в системе сотовой связи GSM»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №4 «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №5 «Исследование методов защиты терминала беспроводной связи Bluetooth»	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение практического задания №1 «Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления»	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»

Выполнение практического задания №2 «Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности»	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Выполнение практического задания №3 «Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений»	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Выполнение практического задания №4 «Методы сигнальной помехозащиты радиолиний»	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Выполнение практического задания №5 «Оценка помехозащиты спутниковой линии связи»	1	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Выполнение практического задания №6 «Оценка эффективности применения методов повышения скрытности РЭС»	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
СРС	8		20	
ИТОГО	24		48	
Посещаемость	0		16	
Зачёт	0		36	
ИТОГО	24		100	

Итоговый контроль – зачёт в форме бланкового тестирования из 15 вопросов. Каждый вопрос на зачёте оценивается в 2,4 балла, итоговая сумма округляется до целого значения, максимальная оценка 36 по зачету.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная и дополнительная учебная литература

1) Сети и системы передачи информации: телекоммуникационные сети [Текст]: учебник и практикум для вузов : [для студентов, обуч. по инженерно-техническим направлениям и специальностям] / К. Е. Самуйлов, И. А. Шалимов, Д. С. Кулябов ; Российский университет дружбы народов. - Москва : Юрайт, 2017. - 363 с. Операционные системы :[Текст] : учебник / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин. – 2-е изд., испр. – М.: Академия, 2012. – 304 с.

2) **Технологии коммутации и** маршрутизации в локальных компьютерных сетях [Текст] : учебное пособие / под общ. ред. А. В. Пролетарского. - Москва : Изд - во МГТУ им. Н. Э. Баумана, 2013. - 389, [3] с. : ил.

8.2Дополнительная литература

1) **Технологии защиты информации** в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - Москва : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.

2) **Олифер, Виктор Григорьевич**. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с.

3) **Крук, Борис Иванович.** Телекоммуникационные системы и сети [Текст] : учебное пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. **Т. 1** : Современные технологии. - 2013. - 620 с. : ил.

4) **Богомолов, С. И.** Введение в системы радиосвязи и радиодоступа [Электронный ресурс] : учебное пособие / С. И. Богомолов. - Томск : Эль Контент, 2012. - 152 с.

5) **Винокуров, В. М.** Цифровые системы передачи [Электронный ресурс] : учебное пособие / В. М. Винокуров. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. - 160 с.

6) **Технические средства и** методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - Москва : Горячая линия - Телеком, 2012. - 616 с. : ил.

7) **Информационная безопасность и** защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

8.3 Перечень методических указаний

1) **Подавление радиосигнала радиопомехой**: методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 6 с.: ил., Библиогр.: с. 6..

2) **Исследование метода защиты речевых сигналов от воздействия широкополосных аддитивных помех:** методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 13 с.. Библиогр.: с. 13..

3) **Исследование методов защиты абонентского терминала в системе сотовой связи GSM:** методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: Библиогр.: с. 10.

4) **Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android:** методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: Библиогр.: с. 10.

5) **Исследование методов защиты терминала беспроводной связи Bluetooth:** методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 9 с.: Библиогр.: с. 8.

6) **Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления:** методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 12 с.: ил., Библиогр.: с. 12.

7) **Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности:** методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 12 с.: ил., Библиогр.: с. 12.

8) **Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений:** методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 8 с.: ил., Библиогр.: с. 8.

9) **Методы сигнальной помехозащиты радиолиний:** методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: ил., Библиогр.: с. 10.

10) **Оценка помехозащиты спутниковой линии связи:** методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 6 с. Библиогр.: с. 6.

11) **Оценка эффективности применения методов повышения скрытности РЭС:** методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 14 с. Библиогр.: с. 14.

8.4 Другие учебно-методические материалы

Отраслевые научно-технические журналы в библиотеке университета:
Проблемы информационной безопасности. Компьютерные технологии.
Защита информации. Инсайд.
Информационные системы и технологии.
Вестник компьютерных и информационных технологий

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Электронная библиотека ЮЗГУ (http://www.lib.swsu.ru)
2. Электронно-библиотечная система «Университетская библиотека online»
3. (http://www.biblioclub.ru)
4. Федеральное хранилище Единая коллекция цифровых образовательных ресурсов (http://school-collection.edu.ru)
5. Федеральный портал Российское образование (http://www.edu.ru)
6. Электронная библиотека образовательных и просветительных изданий (http://www.iqlib.ru)
7. Научная электронная библиотека «Elibrary» (http://elibrary.ru/defaultx.asp)
8. Официальный сайт компании «Консультант Плюс» (http://www.consultant.ru)

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Защита информации в системах беспроводной связи» являются лекции, практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются

рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному и практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информации в системах беспроводной связи»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Защита информации в системах беспроводной связи» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Защита информации в системах беспроводной связи» -

закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Libreoffice (Бесплатная, GNU General Public License) - https://ru.libreoffice.org/ ;
Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. С ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,
Операционная система Windows, договор IT000012385;
Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234;
Oracle Virtualbox (Бесплатная, GNU General Public License) - https://www.virtualbox.org/ ;
GNS3 - графический симулятор сети (свободное ПО) - https://www.gns3.com/ ;
Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet (Бесплатная, GNU General Public License) - https://www.wireshark.org/ ;
Ubuntu Linux (Бесплатная, GNU General Public License) - http://ubuntu.ru/.

В качестве материально-технического обеспечения используются мультимедийные средства, для демонстрации компьютерных симуляторов и графических презентационных материалов. В качестве информационных технологий на занятиях применяются обучающие, информационно-поисковые и справочные, расчетные технологии.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска.
Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”.
Проекционный экран на штативе; Мультимедиацентр: ноутбук ASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проектор inFocusIN24+.
Антенна спутниковой связи. Лабораторная установка «Экспериментальное исследование характеристик направленности источника излучения и поляризации простейших источников электромагнитных волн»
Межсетевой экран Netgear STM150EW-100EUS
Роутер ASUS WL-520GC
Маршрутизатор D-Link DFL-860E
Коммутатор TrendNet TE100-S88E + 8 port 10/100 Switch

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

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. 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, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего
	измененных	заме-нённых	анну-лирова н-ных	новых			