Аннотация к рабочей программе дисциплины ««Информационная безопасность телекоммуникационных систем»

Цель преподавания дисциплины

Целью преподавания дисциплины «Информационная безопасность телекоммуникационных систем» является получение студентами знаний о принципах обеспечения информационной безопасности в телекоммуникационных системах, методах оценки и защиты безопасности систем связи.

Задачи изучения дисциплины

- получить знания об основных понятиях информационной безопасности телекоммуникационных систем;

- получить знания об угрозах информационной безопасности и их классификации;

- получить знания о методах оценки телекоммуникационных систем;

- получить знания о системах электросвязи, угрозах их безопасности и методах защиты;

- получить знания о защите речевой информации в канале связи путем преобразования сигнала;

- получить знания об информационной безопасности телефонной связи;

- получить знания о современных криптографических алгоритмах;

- получить знания о защите информации в системах волоконно-оптической связи;

- получить знания о виртуальных частных сетях.

Компетенции, формируемые в результате освоения дисциплины

Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности (ПК-10).

Разделы дисциплины

Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем». Доктрина информационной безопасности РФ. Угрозы информационной безопасности ТКС. Классификация угроз по компонентам ТКС. Методы оценки уязвимостей ТКС. Системы электросвязи, угрозы безопасности и методы их защиты. Общие методы организации защищенной речевой связи в телефонной сети. Методы защиты информации в телефонном канале связи. Рекомендации по ограничению физического доступа к оборудованию связи. Защита речевой информации в канале связи путем преобразования сигнала. Информационная безопасность телефонной связи. Современные криптографические алгоритмы. Защита информации в системах волоконно-оптической связи. Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС. Пути утечки информации из ВОЛС. Методы защиты информации, передаваемой по ВОЛС. Защита ВОЛС. Виртуальные частные сети.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И. о. декана факультета
фундаментальной и прикладной информатики.
(наименование ф-та полностью)

_____ М.О. Таныгин
(подпись, инициалы, фамилия)

«_31_» _____08_____ 20_21_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность телекоммуникационных систем
(наименование дисциплины)

ОПОП ВО10.05.02Информационная безопасность телекоммуникационных систем
шифр и наименование направления подготовки (специальности)

«Управление безопасностью телекоммуникационных сетей и систем»
наименование направленности (профиля, специализации)

форма обучения_____очная_____
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по специальности10.05.02 Информационная безопасность телекоммуникационных системна основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность специализация «Управление безопасностью телекоммуникационных сетей и систем», одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем» на заседании кафедры информационной безопасности №1 «30» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Ефремов М.А.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем» одобренного Ученым советом университета протокол № 6 «26» 02 2021 г. на заседании кафедры 26, протокол №11 от 30.06.2022 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой М.О. Таныгин

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем», одобренного Ученым советом университета протокол № «___» _____ 20__ г. на заседании кафедры _____
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем», одобренного Ученым советом университета протокол № «___» _____ 20__ г. на заседании кафедры _____
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины.Перечень планируемых результатовобучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность телекоммуникационных систем» является получение студентами знаний о принципах обеспечения информационной безопасности в телекоммуникационных системах, методах оценки и защиты безопасности систем связи.

1.2 Задачи дисциплины

- получить знания об основных понятиях информационной безопасности телекоммуникационных систем;
- получить знания об угрозах информационной безопасности и их классификации;
- получить знания о методах оценки телекоммуникационных систем;
- получить знания о системах электросвязи, угрозах их безопасности и методах защиты;
- получить знания о защите речевой информации в канале связи путем преобразования сигнала;
- получить знания об информационной безопасности телефонной связи;
- получить знания о современных криптографических алгоритмах;
- получить знания о защите информации в системах волоконно-оптической связи;
- получить знания о виртуальных частных сетях.

1.3 Перечень планируемых результатовобучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-10	Способен эксплуатировать средства обеспечения информаци-	ПК – 10.1Проверяет корректность работы программных компо-	***Знать:*** общие характеристики телекоммуникационных систем.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	онной безопасности для реализации политик безопасности	нент телекоммуникационной системы	***Уметь:*** оценивать уровень безопасности телекоммуникационных систем. ***Владеть:*** методами защиты информации систем связи.
		ПК – 10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты	***Знать:***требования профиля защиты для текущего функционала систем. ***Уметь:*** сопоставлять доступные функции системы с требованиями информационной безопасности. ***Владеть:*** методами защиты речевой информации в канале связи путем преобразования сигнала.
		ПК – 10.3 Формирует систематизированные политики информационной безопасности	***Знать:***основные аспекты инфокоммуникационной безопасности телекоммуникационных систем. ***Уметь:*** систематизировать политики информационной безопасности в системе защиты. ***Владеть:***навыками работы с изменениями в политике документации информационной безопасности
		ПК – 10.4 Разрабатывает профили заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении	***Знать:***основные угрозы аспектам инфокоммуникационной безопасности телекоммуникационных систем связи; ***Уметь:***классифицировать угрозы безопасности и их влияние на работу телекоммуникационных систем; ***Владеть:***навыками разработки профилей заданий по безопасности для оборудования теле-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			коммуникационных систем

2Указание местадисциплины в структуре основной профессиональной образовательной программы

Дисциплина«Информационная безопасность телекоммуникационных систем» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы специалитета10.05.02 Информационная безопасность телекоммуникационных систем специализация «Управление безопасностью телекоммуникационных сетей и систем».Дисциплина изучается на 5 курсе в 10 семестре.

3Объем 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 трудоемкость (объем) дисциплины составляет 5 зачетных единиц (з.е.), 180академических часов.

Таблица 3 - Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	85.15
в том числе:	
лекции	42
лабораторные занятия	42
практические занятия	0
Самостоятельная работа обучающихся (всего)	67.85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всегоАттКР)	1.15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1.15

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

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»	Понятие информации, конфиденциальная и открытая информация, информационная безопасность, защита информации, утечка информации, защита информации от несанкционированного доступа, телекоммуникационные системы, отличие дисциплин «Информационная безопасность» и «Информационная безопасность телекоммуникационных систем».
2	Доктрина информационной безопасности РФ	Доктрина информационной безопасности Российской Федерации, типы угроз информационной безопасности Российской Федерации, правовые, организационно-технические и экономические методы обеспечения ИБ РФ.
3	Угрозы информационной безопасности ТКС	Угроза, атака, злоумышленник, уязвимость ТКС, окно опасности, классификация угроз по аспекту информационной безопасности, основные угрозы доступности, основные угрозы целостности, основные угрозы конфиденциальности
4	Классификация угроз по компонентам ТКС	Три класса угроз передачи информации в ТКС, классификации угроз по компонентам ТКС,информационные угрозы.
5	Методы оценки уязвимостей ТКС	Тестирование ТКС, тестирование и оценивание безопасности, тестирование на проникновение, идентификация потенциальных сбоев, уязвимости системы.
6	Системы электросвязи, угрозы безопасности и методы их защиты	Системы телефонной связи, организационные проблемы.
7	Общие методы организации защищенной речевой связи в телефонной сети	Стационарные абоненты, пеший режим, блуждающий режим, подвижный режим.
8	Методы защиты информации в телефонном канале связи	Методы, основанные на ограничении физического доступа к линии и аппаратуре связи, и методы, основанные на преобразовании сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.
9	Рекомендации по ограничению физического доступа к оборудованию связи	Правила организации рабочего места абонента защищенной связи.

10	Защита речевой информации в канале связи путем преобразования сигнала	Аппаратура защиты с кодированием голоса, аппаратура защиты с кодированием звуковых сигналов на скорости 30-64 кбит/сек с последующим шифрованием полученного цифрового потока, преобразования с временными или частотными перестановками (скремблированием) с переменными перестановками под управлением криптоблока и комбинированные мозаичные преобразования, преобразования с временными перестановками (скремблированием) и временной инверсией элементов речевого сигнала со статическим законом перестановки, преобразования с инверсией спектра и статическими перестановками спектральных компонент речевого сигнала.
11	Информационная безопасность телефонной связи	Краткая характеристика систем телефонной связи, пути и места утечки информации в телефонных системах, каналы побочной утечки телефонной информации, основные методы защиты информации, скремблирование сигнала и шифрование цифровой информации, варианты подключения шифрующих устройств.
12	Современные криптографические алгоритмы	Общая характеристика криптографических систем, Классические алгоритмы шифрования, шифрование по стандарту DES, асимметричные криптосистемы, использование генератора псевдослучайных чисел.
13	Защита информации в системах волоконно-оптической связи	Особенности оптических систем связи, физические особенности, технические особенности, недостатки волоконной технологии.
14	Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС	Поляризационная модовая дисперсия, внешние факторы воздействия на величину ПМД, быстрые и медленные состояниями поляризации PSP
15	Пути утечки информации из ВОЛС	Пути утечки информации,основные физические принципы формирования каналов утечки в ВОЛС, способы формирования каналов утечки излучений из ВОЛС, способы осуществления несанкционированного доступа к ВОЛС.
16	Методы защиты информации, передаваемой по ВОЛС	Физические методы защиты, разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ, СДС с анализом прошедшего сигнала, СДС с анализом отраженного сигнала, краткий обзор криптографических методов защиты, пример использования криптографического метода защиты.
17	Защита ВОЛС	Три основных направления защиты, кодовое зашумления передаваемых сигналов, метод создания и контроля картины интерференции, метод анализамодового состава, метод режима динамического хаоса, механические и электрические средства защиты, датчики контроля подключения к оптическому кабелю, метод частотно-модулированного зондирования, метод защиты с использованием многослойного оптическоговолокна со специальной структурой, квантовая криптография.
18	Виртуальные частные сети	VPN-соединение, туннель, канал доступа, виды VPN, безопасность VPN, атаки на VPN, преимущества VPN, возможности VPN.

Таблица 4.1.2 –Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел учебной дисциплины	Виды учебной деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек.	№ лаб.	№ пр.			
1	Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»	21	-	-	О – 1 Д – 3, 4	С2	ПК-10.1
2	Доктрина информационной безопасности РФ	21	-	-	О – 1 Д – 3, 4	С2	ПК-10.1
3	Угрозы информационной безопасности ТКС	21	-	-	О – 1 Д – 1, 2	С3	ПК-10.2
4	Классификация угроз по компонентам ТКС	21	-	-	О – 1 Д – 2, 3	С4	ПК-10.3
5	Методы оценки уязвимостей ТКС	21	-	-	О – 2 Д – 5, 6	С5	ПК-10.3
6	Системы электросвязи, угрозы безопасности и методы их защиты	21	1	-	О – 2 Д – 5 МУ – 1	С6, КО6	ПК-10.1
7	Общие методы организации защищенной речевой связи в телефонной сети	21	2	-	О – 2 Д – 7 МУ – 2	С7, КО7	ПК-10.4
8	Методы защиты информации в телефонном канале связи	21	3	-	О – 2 Д – 6 МУ – 3	С8, КО8	ПК-10.2
9	Рекомендации по ограничению физического доступа к оборудованию связи	21	4	-	О – 2 Д – 7 МУ – 4	С9, КО9	ПК-10.3
10	Защита речевой информации в канале связи путем преобразования сигнала	21	5	-	О – 2 Д – 3 МУ – 5	С10, КО10	ПК-10.4
11	Информационная безопасность телефонной связи	21	6	-	О – 1 Д – 1 МУ – 6	С11, КО11	ПК-10.3
12	Современные криптографические алгоритмы	21	-	-	О – 1 Д – 2, 4	С12	ПК-10.2
13	Защита информации в системах волоконно-оптической связи	21	-	-	О – 2 Д – 4, 6	С13	ПК-10.2
14	Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС	21	-	-	О – 1 Д – 6	С14	ПК-10.3

15	Пути утечки информации из ВОЛС	21	-	-	О – 1 Д – 5	С15	ПК-10.1 ПК-10.3
16	Методы защиты информации, передаваемой по ВОЛС	21	-	-	О – 2 Д – 7	С16	ПК-10.2
17	Защита ВОЛС	21	-	-	О – 2 Д – 7	С17	ПК-10.3
18	Виртуальные частные сети	21	-	-	О – 1 Д – 6, 7	С18	ПК-10.4

С – собеседование, Т – тест, Р – реферат, КО – контрольный опрос.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Практическая работа №1 «Общие вопросы обработки сигналов в программе Adobe Audition»	6
2	Практическая работа №2 «Маскировка тонального телефонного сигнала путем его зашумления»	6
3	Практическая работа №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»	6
4	Практическая работа №4 «Обработка тональных сигналов набора номера»	8
5	Практическая работа №5 «Модификация тонального сигнала набора номера»	8
6	Практическая работа №6 «Маскировка телефонного сигнала методом статической перестановки его временных сегментов»	8
Итого		42

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельнаяработа студентов

№ раздела (темы)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»	1неделя	2
2.	Доктрина информационной безопасности РФ	2 неделя	2
3.	Угрозы информационной безопасности ТКС	3 неделя	4
4.	Классификация угроз по компонентам ТКС	4 неделя	4
5.	Методы оценки уязвимостей ТКС	5 неделя	4
6.	Системы электросвязи, угрозы безопасности и методы их защиты	6 неделя	4

7.	Общие методы организации защищенной речевой связи в телефонной сети	7 неделя	4
8.	Методы защиты информации в телефонном канале связи	8 неделя	4
9.	Рекомендации по ограничению физического доступа к оборудованию связи	9 неделя	4
10.	Защита речевой информации в канале связи путем преобразования сигнала	10 неделя	4
11.	Информационная безопасность телефонной связи	11 неделя	4
12.	Современные криптографические алгоритмы	12 неделя	4
13.	Защита информации в системах волоконно-оптической связи	13 неделя	4
14.	Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС	14 неделя	4
15.	Пути утечки информации из ВОЛС	15 неделя	4
16.	Методы защиты информации, передаваемой по ВОЛС	16 неделя	4
17.	Защита ВОЛС	17 неделя	4
18.	Виртуальные частные сети	18 неделя	3,85
Итого			67.85

5Перечень 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 УП и 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 разработки:

– методических рекомендаций, пособий по организации самостоятельной ра-

боты студентов;

– тем рефератов;

– вопросов к зачету;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6Образовательные 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 универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных практикоориентированных заданий.

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
1	Практическая работа №1 «Общие вопросы обработки сигналов в программе Adobe Audition»	Выполнение студентом интерактивных заданий в программе AdobeAudition.	2
2	Практическая работа №2 «Маскировка тонального телефонного сигнала путем его зашумления»	Выполнение студентом интерактивных заданий по маскировке тонального телефонного сигнала.	2
3	Практическая работа №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»	Выполнение студентом интерактивных заданий по определению неизвестного номера абонента.	2
4	Практическая работа №4 «Обработка тональных сигналов набора номера»	Выполнение студентом интерактивных заданий по обработке тональных сигналов набора номера.	2
Итого:			8

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, экономическому, 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, высокого профессионализма ученых, 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.

7Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональнойобразовательной программы

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули)и практики, при изучении/ прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК – 10.1Проверяет корректность работы программных компонент телекоммуникационной системы	Инфокоммуникационные системы навигации и диспетчеризации и их защита Безопасность средств мониторинга территорий и объектов		Информационная безопасность телекоммуникационных систем Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 10.2 Определяет соответствие текущего	Инфокоммуникационные системы навигации и диспетчеризации и их защита		Информационная безопасность телекоммуникационных систем

функционала системы требованиям профилей защиты	Безопасность средств мониторинга территорий и объектов	Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 10.3 Формирует систематизированные политики информационной безопасности	Инфокоммуникационные системы навигации и диспетчеризации и их защита Безопасность средств мониторинга территорий и объектов	Информационная безопасность телекоммуникационных систем Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 10.4 Разрабатывает профили заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении	Инфокоммуникационные системы навигации и диспетчеризации и их защита Безопасность средств мониторинга территорий и объектов	Информационная безопасность телекоммуникационных систем Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-10 завершающий	ПК – 10.1 Проверяет корректность работы программных компонент телекоммуникационной системы	**Знать**: основное понятие ИБ ТКС, основные её функции **Уметь**: анализировать научно-техническую информацию ИБ ТКС. **Владеть (или Иметь опыт деятельности):**: оценки различных компонентов подсистем обеспечения ИБ ТКС.	**Знать**: принципы организации подсистем безопасности ТКС. **Уметь**: анализировать научно-техническую информацию и нормативные материалы ИБ ТКС. **Владеть (или Иметь опыт деятельности):**: составления аналитического отчета о состоянии ИБ ТКС.	**Знать**: критерии соответствия функционала подсистем информационной безопасности ТКС угрозам для объектов информатизации. **Уметь**: анализировать научно-техническую информацию и нормативные и методические материалы ИБ ТКС. **Владеть (или Иметь опыт деятельности):**: составления методических комплексов по ИБ ТКС.

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	ПК – 10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты	**Знать**: основное понятие ИБ ТКС, основные её функции **Уметь**: анализировать научно-техническую информацию ИБ ТКС. **Владеть (или Иметь опыт деятельности):**: оценки различных компонентов подсистем обеспечения ИБ ТКС.	**Знать**: принципы организации подсистем безопасности ТКС. **Уметь**: анализировать научно-техническую информацию и нормативные материалы ИБ ТКС. **Владеть (или Иметь опыт деятельности):**: составления аналитического отчета о состоянии ИБ ТКС.	**Знать**: критерии соответствия функционала подсистем информационной безопасности ТКС угрозам для объектов информатизации. **Уметь**: анализировать научно-техническую информацию и нормативные и методические материалы ИБ ТКС. **Владеть (или Иметь опыт деятельности):**: составления методических комплексов по ИБ ТКС.
	ПК – 10.3 Формирует систематизированные политики информационной безопасности	**Знать**: основное понятие ИБ ТКС, основные её функции **Уметь**: выполнять сервисные мероприятия с системами программно-аппаратной защиты информации ТКС. **Владеть (или Иметь опыт деятельности):**: эксплуатации различных компонентов подсистем обеспечения ИБ ТКС.	**Знать**: принципы организации подсистем безопасности ТКС. **Уметь**: настраивать программно-аппаратные системы защиты информации ТКС. **Владеть (или Иметь опыт деятельности):**: администрирования программно-аппаратных СЗИ ТКС.	**Знать**: критерии соответствия функционала подсистем информационной безопасности ТКС угрозам для объектов информатизации. **Уметь**: выбирать требуемы политики безопасности при настройке программно-аппаратных СЗИ. **Владеть (или Иметь опыт деятельности):**: реагировании на нештатные ситуации, возникающие при эксплуатации программно-аппаратных СЗИ

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				ТКС.
	ПК – 10.4 Разрабатывает профили заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении	***Знать:*** типы оборудования телекоммуникационных систем ***Уметь:*** разграничивать оборудование в зависимости от профиля задания по безопасности ***Владеть (****или* ***Иметь опыт деятельности): навыками работы с документацией конфиденциального характера***	***Знать:***профили заданий по безопасности ***Уметь:***различать профили документации по безопасности в системах защиты ***Владеть (****или* ***Иметь опыт деятельности):***навыками проверки степени защищённости документации	***Знать:***обеспечение объекта оборудованием телекоммуникационных систем в защищённом исполнении ***Уметь:***подбирать для каждого типа оборудования свои способы обеспечения безопасности ***Владеть (****или* ***Иметь опыт деятельности): в*** разработке профилей заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении

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 основной профессиональнойобразовательной программы

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля-успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируе-	Технология формирова-	Оценочные средства	Описание шкал оценивания

		мой компетенции (или ее части)	ния	наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»	ПК-10.1	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
2	Доктрина информационной безопасности РФ	ПК-10.1	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
3	Угрозы информационной безопасности ТКС	ПК-10.2	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
4	Классификация угроз по компонентам ТКС	ПК-10.3	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
5	Методы оценки уязвимостей ТКС	ПК-10.3	Лекция, СРС	Собеседование	1-3	Согласно табл.7.2
6	Системы электросвязи, угрозы безопасности и методы их защиты	ПК-10.1	Лекция, СРС, практическое занятие	Собеседование	1-3	Согласно табл.7.2
				Контрольные вопросы к ПР№1	1-14	
7	Общие методы организации защищенной речевой связи в телефонной сети	ПК-10.4	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ПР№2	1-3	
8	Методы защиты информации в телефонном канале связи	ПК-10.2	Лекция, СРС, практическое занятие	Собеседование	1-4	Согласно табл.7.2
				Контрольные вопросы к ПР№3	1-5	

9	Рекомендации по ограничению физического доступа к оборудованию связи	ПК-10.3	Лекция, СРС, практическое занятие	Собеседование	1-5	Согласно табл.7.2
				Контрольные вопросы к ПР№4	1-6	
10	Защита речевой информации в канале связи путем преобразования сигнала	ПК-10.4	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ПР№5	1-10	
11	Информационная безопасность телефонной связи	ПК-10.3	Лекция, СРС, практическое занятие	Собеседование	1-6	Согласно табл.7.2
				Контрольные вопросы к ПР№6	1-8	
12	Современные криптографические алгоритмы	ПК-10.2	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
13	Защита информации в системах волоконно-оптической связи	ПК-10.2	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
14	Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС	ПК-10.3	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
15	Пути утечки информации из ВОЛС	ПК-10.1 ПК-10.3	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
16	Методы защиты информации, передаваемой по ВОЛС	ПК-10.2	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2
17	Защита ВОЛС	ПК-10.3	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2

18	Виртуальные частные сети	ПК-10.4	Лекция, СРС	Собеседование	1-6	Согласно табл.7.2

Примеры типовых контрольных заданий для проведения текущего контроляуспеваемости

Вопросы собеседования по разделу (теме) 1. «Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»».

1. Что такое информация?
2. На какие группы подразделяют виды информации?
3. Что такое информационная безопасность?
4. Что понимается под утечкой информации?
5. На какие системы разделяют системы передачи информации?
6. Как называется информация, предназначенная для использования ограниченным кругом лиц?

Контрольные вопросы к лабораторной работе по теме «Обработка тональных сигналов набора номера»

1. Привести схему нерайонированной и районированной ГТС.
2. Что такое сигнализация, система сигнализации и протокол сигнализации.
3. Привести виды сигнализации в телефонных сетях по их функциональному назначению.
4. Привести классы систем межстанционной сигнализации.
5. Какие используются виды кодирования набора номера.
6. Чем характеризуются импульсный и тональный наборы номера.

Полностью оценочные материалыи оценочные средства дляпроведения текущего контроля успеваемостипредставлены в УММ подисциплине.

Типовые задания для проведенияпромежуточной аттестацииобучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы изадания 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.БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

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(или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных 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.

Примеры типовых заданий для проведения промежуточной аттестацииобучающихся

Задание в закрытой форме:

_____принято называть информацию, отнесенную к государственной тайне, сохранность которой регламентируется соответствующими законами, за разглашение которой установлена уголовная ответственность.

Задание в открытой форме:

Доктрина информационной безопасности Российской Федерации была утверждена:

- 9 марта 2012 года;
- 9 февраля 2002 года;
- 9 сентября 2000 года;
- 9 декабря 1998 года.

Задание на установление правильной последовательности:

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

1) заплаты должны быть установлены в защищаемой ИС.
2) должно стать известно о средствах использования пробела в защите;
3) должны быть выпущены соответствующие заплаты.

Задание на установление соответствия:

1) правовыеметоды обеспечения информационной безопасности;
2) организационно-техническиеметоды обеспечения информационной безопасности;
3) экономическиеметоды обеспечения информационной безопасности.

А)выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

Б) совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц;

В)разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Компетентностно-ориентированная задача:

Определение неизвестного номера абонента путем спектральной оценки частотных параметров тональных сигналов набора этого номерав программе Adobe Audition.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихсяпредставлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

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

– положение П 02.016–2018Обалльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

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

Для *текущего контроляуспеваемости*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
1	2	3	4	5
Лабораторная работа №1 «Общие вопросы обработки сигналов в программе Adobe Audition»;	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Лабораторная работа №2 «Маскировка тонального телефонного сигнала путем его зашумления»;	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Лабораторная работа №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»;	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Лабораторная работа №4 «Обработка тональных сигналов набора номера»;	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Лабораторная работа №5 «Модификация тонального сигнала набора номера»;	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Лабораторная работа №6 «Маскировка телефонного сигнала методом статической перестановки его временных сегментов»;	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
СРС	8		24	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для промежуточной аттестацииобучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности.В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированнойзадачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная учебная литература

1) Сети и системы передачи информации: телекоммуникационные сети : 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. - Текст : непосредственный.

2) Синицын, Сергей Владимирович. Операционные системы : учебник / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин. – 2-е изд., испр. – М.: Академия, 2012. – 304 с. - Текст : непосредственный.

3) Винокуров, В. М. Цифровые системы передачи : учебное пособие / В. М. Винокуров. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. - 160 с. - URL: http://biblioclub.ru/index.php?page=book&id=209018 (дата обращения 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

8.2 Дополнительная литература

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

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

3) Крук, Борис Иванович. Телекоммуникационные системы и сети : 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. - Текст : непосредственный.

4) Богомолов, С. И. Введение в системы радиосвязи и радиодоступа : учебное пособие / С. И. Богомолов. - Томск : Эль Контент, 2012. - 152 с. - URL: http://biblioclub.ru/index.php?page=book&id=208609 (дата обращения 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

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

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

8.3 Перечень методических указаний

1) Общие вопросы обработки сигналов в программе Adobe Audition : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 14 с. - Текст : электронный.

2) Маскировка тонального телефонного сигнала путем его зашумления : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

3) Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 11 с. - Текст : электронный.

4) Обработка тональных сигналов набора номера : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 13 с. - Текст : электронный.

5) Модификация тонального сигнала набора номера : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 11 с. - Текст : электронный.

6) Маскировка телефонного сигнала методом статической перестановки его временных сегментов : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 12 с. - Текст : электронный.

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», необходимых для освоения дисциплины

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)

10Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность телекоммуникационных систем» являются лекции 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 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 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.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Информационная безопасность телекоммуникационных систем»: 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, отработкустудентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы 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 закрепленияосвоенного 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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность телекоммуникационных систем» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность телекоммуникационных систем» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

1) Libreoffice (Бесплатная, GNU General Public License) - https://ru.libreoffice.org/ ;
2) 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»;
3) Операционная система Windows, договор IT000012385;
4) Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234;
5) Adobe Audition (Бесплатная пробная версия) - https://creative.adobe.com/ru/products/download/audition .

12Описание 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) Компьютер NORBEL C239264Ц-AMD/2x8Gb/2TB/DVDRW/LCD 20";

– Система виброакустического зашумления «Шорох-2», виброакустический датчик КПВ-2, акустический излучатель OMS -2000
– Подавитель «жучков» и беспроводных видеокамер “BigHunter Spy”
– Комбинированный поисковый прибор “D008”
– Генератор шума Соната-С1

Для проведения промежуточной аттестации необходимо следующее материально-техническое оборудование:

1. Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24

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 такжесурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменноотвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). 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).

14Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			