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

Утверждаю
Зам. директора по УВР
_____ Н.А.Андреева
«24» 05 2024 г.

Б1.О.24 Основы информационной безопасности
рабочая программа дисциплины

Кафедра Инфокоммуникационные технологии и системы связи
Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль: **Защищенные инфокоммуникационные системы (ЗИКС), Инфокоммуникационные системы и сети (ИКСиС)**

Формы обучения **очная, очно-заочная, заочная**

Распределение часов дисциплины по семестрам (для очной и очно-заочной формы обучения (ОФО и ОЗФО)), курсам (для заочной формы обучения (ЗФО))

Объем и структура учебной практики по семестрам (ОФО и ОЗФО), курсам (ЗФО)										
	ЗИКС				**ИКСиС**					
Вид учебной работы	ОФО		ЗФО		ОФО		ЗФО		ОЗФО	
	ЗЕ	часов	ЗЕ	часов	ЗЕ	часов	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	2	72/5	2	72/3	2	72/5	2	72/3	2	72/5
Контактная работа, в том числе (по семестрам, курсам):		32/5		12/3		32/5		12/3		14/5
Лекции		16/5		2/2 4/3		16/5		2/2 4/3		6/5
Лабораторных работ										
Практических занятий		16/5		6/3		16/5		6/3		8/5
Семинаров										
Самостоятельная работа		40/5		60/3		40/5		60/3		58/5
Контроль										
Число контрольных работ (по курсам)										
Число КР (по семестрам, курсам)										
Число КП (по семестрам, курсам)										
Число зачетов с разбивкой по семестрам		1/5		1/3		1/5		1/3		1/5
Число экзаменов с разбивкой по семестрам (курсам)										

Программу составил:
Профессор кафедры ИТСС, д.п.н., доцент Жуковский А.Г.

Рецензент:
Ведущий научный сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Основы информационной безопасности»

разработана в соответствии с ФГОС ВО:
Федеральным государственным образовательным стандартом высшего образования, направление подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

Составлена на основании учебных планов
направления 11.03.02 Инфокоммуникационные технологии и системы связи, профиля «Инфокоммуникационные системы и сети», одобренных Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденных директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «20» 05 2024 г. № 10

Зав. кафедрой _____ В.И. Юхнов

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

Утверждаю
Зам. директора по УВР _____
«___» _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _____ 20__ г. № ____
Зав. кафедрой _____

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

Утверждаю
Зам. директора по УВР _____
«___» _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _____ 20__ г. № ____
Зав. кафедрой _____

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

Утверждаю
Зам. директора по УВР _____
«___» _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _____ 20__ г. № ____
Зав. кафедрой _____

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

Утверждаю
Зам. директора по УВР _____
«___» _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _____ 20__ г. № ____
Зав. кафедрой _____

1. Цели изучения дисциплины

Целью преподавания дисциплины «Основы информационной безопасности сетей и систем» является формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***технологическим*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-3: Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности
Знать:
основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и трактам телекоммуникационных систем; принципы, основные алгоритмы и устройства цифровой обработки сигналов; принципы построения телекоммуникационных систем различных типов и способы распределения информации в сетях связи;
Уметь:
решать задачи обработки данных с помощью средств вычислительной техники; строить вероятностные модели для конкретных процессов, проводить необходимые расчеты в рамках построенной модели;
Владеть:
методами и навыками обеспечения информационной безопасности;

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Основы информационной безопасности сетей и систем» является логическим продолжением дисциплины Б1.О.07 «Информатика», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Основы информационной безопасности сетей и систем» базируется также на знаниях, приобретенных из дисциплин: Б1.О.03 Иностранный язык, Б1.О.04 Высшая математика, Б1.О.05 Теория вероятностей и математическая статистика, Б1.О.06 Дискретная математика.
3	Б1.О.13 «Основы построения инфокоммуникационных систем и сетей»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин Б1.В.11 «Основы криптографии», Б1.В.14 «Методы и средства защиты компьютерной информации», Б1.В.ДВ.05.01 «Технические средства и методы защиты информации», а также других дисциплин и практик, формирующих общепрофессиональные и профессиональные компетенции и связанных с защитой информации.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 72 часов, 32 аудиторных часов, 40 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 2, Семестр 3					
Модуль 1. Понятие информационной безопасности. Основные составляющие и направления обеспечения информационной безопасности. 38 часов (18+20) часов					
1.1	Лекция 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Основные концептуальные положения системы защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией	Л1.	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита	Л2.	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 5.1.Общие положения 5.2.Защита информации от утечки по визуально оптическим каналам 5.3.Защита информации от утечки по акустическим каналам 5.4.Защита информации от утечки по электромагнитным каналам 5.5.Защита информации от утечки по материально - вещественным каналам	Л3.	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Правовая защита от компьютерных преступлений и защита интеллектуальной собственности.	ПЗ1	2	ОПК-3	Л3.1
1.5	Практическое занятие №2. Противодействие несанкционированному доступу к источникам конфиденциальной информации 1. Способы несанкционированного доступа 2. Технические средства несанкционированного доступа к информации 3. Защита от наблюдения и фотографирования 4. Защита от подслушивания 5. Противодействие незаконному подключению к линиям связи	ПЗ2	2	ОПК-3	Л3.1

	6. Защита от перехвата.				
1.6	Лекция 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 1. Классификация методов криптографического преобразования информации 2. Шифрование. Основные понятия 3. Методы шифрования с симметричным ключом 4. Системы шифрования с открытым ключом 5. Стандарты шифрования 6. Перспективы использования криптозащиты информации в КС.	Л4	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.7	Практическое занятие №3. Технические средства обеспечения информационной безопасности 1. Поисковое оборудование. 2. Технические средства активного и пассивного противодействия нарушениям информационной безопасности.	ПЗ3	2	ОПК-3	Л3.1
1.8	Практическое занятие №4. Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	ПЗ4	2	ОПК-3	Л3.2
1.9	Практическое занятие №5. Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	ПЗ5	2	ОПК-3	Л3.2
1.10	Характеристика защитных действий; Пресечение разглашения конфиденциальной информации; «Исследование алгоритма симметричной системы шифрования данных – стандарт ГОСТ 28147-89». «Изучение алгоритма открытого распределения ключей Диффи-Хелмана». «Изучение алгоритма ассиметричной (двухключевой) системы шифрования данных RSA». Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации. Перечень сведений, отнесенных к государственной тайне. Указ президента российской федерации о перечне сведений, отнесенных к государственной тайне. 24 января 1998 года № 61. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 200 2 г. № 290.	СРС	20	ОПК-3	Л1.1 Л1.2 Л1.3

	Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.				
Модуль 2. Комплексная защита информации в инфокоммуникационных системах и сетях 34 часов (14+20)					
2.1	Лекция 5. СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.	Л5	4	ОПК-3	Л1.1 Л1.2 Л1.3
2.2	Практическое занятие №6. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам	ПЗ6	2	ОПК-3	Л3.2
2.3	Лекция 6. КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕХАНИЗМЫ БОРЬБЫ С НИМИ 1. Классификация компьютерных вирусов 2. Файловые вирусы 3. Загрузочные вирусы 4. Вирусы и операционные системы 5. Методы и средства борьбы с вирусами 6. Профилактика заражения вирусами компьютерных 7. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами	Л6	2	ОПК-3	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие №7. Исследование характеристик и возможностей антивирусного ПО	ПЗ7	2	ОПК-3	Л3.2
2.5	Лекция 7. ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ ОТ ПОТЕРИ ИНФОРМАЦИИ И НАРУШЕНИЙ РАБОТОСПОСОБНОСТИ СЕТЕЙ И СИСТЕМ 1. Внесение функциональной и информационной избыточности. 2. Способы резервирования информации; правила обновления резервных данных. 3. Методы сжатия информации; архивация файловых данных; резервирование системных данных; подготовка к программной среде.	Л7	2	ОПК-3	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие №8. Исследование характеристик и возможностей программ по восстановлению потерянных данных	ПЗ8	2	ОПК-3	Л3.2

2.7	Исследование характеристик и возможностей программ по организации резервного копирования	СРС	4	ОПК-3	Л3.2
2.8	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных	СРС	16	ОПК-3	Л1.1 Л1.2 Л1.3
Итого – 72 часов					

4.2 Заочная форма обучения (всего 72 часов, аудиторных 12 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3					
Модуль 1. Понятие информационной безопасности. Основные составляющие и направления обеспечения информационной безопасности. 36 часов (8+28) часов					
1.1	Лекция 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Основные концептуальные положения системы защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией	СРС	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита	Л2	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 5.1.Общие положения 5.2.Защита информации от утечки по визуально оптическим каналам 5.3.Защита информации от утечки по акустическим	СРС	4	ОПК-3	Л1.1 Л1.2 Л1.3

	каналам 5.4.Защита информации от утечки по электромагнитным каналам 5.5.Защита информации от утечки по материально - вещественным каналам				
1.4	Практическое занятие №1 Правовая защита от компьютерных преступлений и защита интеллектуальной собственности.	ПЗ1	2	ОПК-3	Л3.1
1.5	Практическое занятие №2. Противодействие несанкционированному доступу к источникам конфиденциальной информации 1. Способы несанкционированного доступа 2. Технические средства несанкционированного доступа к информации 3. Защита от наблюдения и фотографирования 4. Защита от подслушивания 5. Противодействие незаконному подключению к линиям связи 6. Защита от перехвата.	СРС	4	ОПК-3	Л3.1
1.6	Лекция 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 1. Классификация методов криптографического преобразования информации 2. Шифрование. Основные понятия 3. Методы шифрования с симметричным ключом 4. Системы шифрования с открытым ключом 5. Стандарты шифрования 6. Перспективы использования криптозащиты информации в КС.	СРС	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.7	Практическое занятие №3. Технические средства обеспечения информационной безопасности 1. Поисковое оборудование. 2. Технические средства активного и пассивного противодействия нарушениям информационной безопасности.	ПЗ3	4	ОПК-3	Л3.1
1.8	Лабораторная работа 1 Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	СРС	2	ОПК-3	Л3.2
1.9	Лабораторная работа 2 Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	СРС	2	ОПК-3	Л3.2
1.10	Характеристика защитных действий; Пресечение разглашения конфиденциальной информации; «Исследование алгоритма симметричной системы шифрования данных – стандарт ГОСТ 28147-89». «Изучение алгоритма открытого распределения ключей Диффи-Хелмана».	СРС	8	ОПК-3	Л1.1 Л1.2 Л1.3

	«Изучение алгоритма ассиметричной (двухключевой) системы шифрования данных RSA». Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации. Перечень сведений, отнесенных к государственной тайне. Указ президента российской федерации о перечне сведений, отнесенных к государственной тайне. 24 января 1998 года № 61. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 200 2 г. № 290. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.				
Модуль 2. Комплексная защита информации в инфокоммуникационных системах и сетях 36 часов (4+32)					
2.1	Лекция 5. СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.	СРС	4	ОПК-3	Л1.1 Л1.2 Л1.3
2.2	Лабораторная работа 3 Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам	СРС	2	ОПК-3	Л3.2
2.3	Лекция 6. КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕХАНИЗМЫ БОРЬБЫ С НИМИ 1. Классификация компьютерных вирусов 2. Файловые вирусы 3. Загрузочные вирусы 4. Вирусы и операционные системы 5. Методы и средства борьбы с вирусами 6. Профилактика заражения вирусами компьютерных	СРС	2	ОПК-3	Л1.1 Л1.2 Л1.3

	7. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами				
2.4	Лабораторная работа 4 Исследование характеристик и возможностей антивирусного ПО	СРС	4	ОПК-3	Л3.2
2.5	Лекция 7. ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ ОТ ПОТЕРИ ИНФОРМАЦИИ И НАРУШЕНИЙ РАБОТОСПОСОБНОСТИ СЕТЕЙ И СИСТЕМ 1. Внесение функциональной и информационной избыточности. 2. Способы резервирования информации; правила обновления резервных данных. 3. Методы сжатия информации; архивация файловых данных; резервирование системных данных; подготовка к программной среде.	Л7	4	ОПК-3	Л1.1 Л1.2 Л1.3
2.6	Лабораторная работа 5 Исследование характеристик и возможностей программ по восстановлению потерянных данных	СРС	4	ОПК-3	Л3.2
2.7	Лабораторная работа 6 Исследование характеристик и возможностей программ по организации резервного копирования	СРС	4	ОПК-3	Л3.2
2.8	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных	СРС	12	ОПК-3	Л1.1 Л1.2 Л1.3
Итого – 72 часов					

4.3 Очно-заочная форма обучения (всего 72 часов, аудиторных 14 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, семестр 5					
Модуль 1. Понятие информационной безопасности. Основные составляющие и направления обеспечения информационной безопасности. 36 часов (8+28) часов					
1.1	КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Основные концептуальные положения системы	СРС	2	ОПК-3	Л1.1 Л1.2 Л1.3

	защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией				
1.2	Лекция 1. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита	Л1	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.3	ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 5.1.Общие положения 5.2.Защита информации от утечки по визуально оптическим каналам 5.3.Защита информации от утечки по акустическим каналам 5.4.Защита информации от утечки по электромагнитным каналам 5.5.Защита информации от утечки по материально - вещественным каналам	СРС	4	ОПК-3	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Правовая защита от компьютерных преступлений и защита интеллектуальной собственности.	ПЗ1	2	ОПК-3	Л3.1
1.5	Противодействие несанкционированному доступу к источникам конфиденциальной информации 1. Способы несанкционированного доступа 2. Технические средства несанкционированного доступа к информации 3. Защита от наблюдения и фотографирования 4. Защита от подслушивания 5. Противодействие незаконному подключению к линиям связи 6. Защита от перехвата.	СРС	4	ОПК-3	Л3.1
1.6	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 1. Классификация методов криптографического преобразования информации 2. Шифрование. Основные понятия 3. Методы шифрования с симметричным ключом 4. Системы шифрования с открытым ключом 5. Стандарты шифрования 6. Перспективы использования криптозащиты информации в КС.	СРС	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.7	Практическое занятие №2. Технические средства обеспечения информационной безопасности 1. Поисковое оборудование. 2. Технические средства активного и пассивного противодействия нарушениям информационной	ПЗ2	4	ОПК-3	Л3.1

	безопасности.				
1.8	Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	СРС	2	ОПК-3	Л3.2
1.9	Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	СРС	2	ОПК-3	Л3.2
1.10	Характеристика защитных действий; Пресечение разглашения конфиденциальной информации; «Исследование алгоритма симметричной системы шифрования данных – стандарт ГОСТ 28147-89». «Изучение алгоритма открытого распределения ключей Диффи-Хелмана». «Изучение алгоритма ассиметричной (двухключевой) системы шифрования данных RSA». Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации. Перечень сведений, отнесенных к государственной тайне. Указ президента российской федерации о перечне сведений, отнесенных к государственной тайне. 24 января 1998 года № 61. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 200 2 г. № 290. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	СРС	8	ОПК-3	Л1.1 Л1.2 Л1.3
Модуль 2. Комплексная защита информации в инфокоммуникационных системах и сетях 36 часов (6+30)					
2.1	СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.	СРС	4	ОПК-3	Л1.1 Л1.2 Л1.3
2.2	Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка	СРС	4	ОПК-3	Л3.2

	подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам				
2.3	КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕХАНИЗМЫ БОРЬБЫ С НИМИ 1. Классификация компьютерных вирусов 2. Файловые вирусы 3. Загрузочные вирусы 4. Вирусы и операционные системы 5. Методы и средства борьбы с вирусами 6. Профилактика заражения вирусами компьютерных 7. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами	СРС	2	ОПК-3	Л1.1 Л1.2 Л1.3
2.4	Исследование характеристик и возможностей антивирусного ПО	СРС	4	ОПК-3	Л3.2
2.5	Лекция 2. ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ ОТ ПОТЕРИ ИНФОРМАЦИИ И НАРУШЕНИЙ РАБОТОСПОСОБНОСТИ СЕТЕЙ И СИСТЕМ 1. Внесение функциональной и информационной избыточности. 2. Способы резервирования информации; правила обновления резервных данных. 3. Методы сжатия информации; архивация файловых данных; резервирование системных данных; подготовка к программной среде.	Л2	4	ОПК-3	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие 3 Исследование характеристик и возможностей программ по восстановлению потерянных данных	ПЗ 3	2	ОПК-3	Л3.2
2.7	Исследование характеристик и возможностей программ по организации резервного копирования	СРС	4	ОПК-3	Л3.2
2.8	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных	СРС	12	ОПК-3	Л1.1 Л1.2 Л1.3
Итого – 72 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Е. Б. Белов, В. Лось, Р. В. Мещеряков, Д. А. Шелупанов	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60x88 1/16. - (Специальность; Учебное пособие для высших учебных заведений.	Э1
Л1.2	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.:Гор. линия-Телеком, 2015. - 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Гатчин Ю.А., Климова Е.В.	Введение в комплексную защиту объектов информатизации	СПб. : Университет ИТМО, 2011. — 112 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/65808.html	Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Шевчук П.С.	Методические указания по проведению практических занятий по дисциплине «Основы информационной безопасности сетей и систем»/ П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 36 с.: ил.	РнД: СКФ МТУСИ, 2016	Э5
Л3.2	Жуковский А.Г., Жуковский Д.А., Швидченко С.А.	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2020. – 52 с.	РнД: СКФ МТУСИ, 2020	Э6

5.2. Электронные образовательные ресурсы	
Э1	http://znanium.com/catalog/product/405159
Э2	http://znanium.com/catalog/product/895240
Э3	https://www.iprbookshop.ru/87995.html
Э4	http://www.iprbookshop.ru/65808.html
Э5	http://www.skf-mtusi.ru/?page_id=659
Э6	http://www.skf-mtusi.ru/?page_id=659

5.3. Программное обеспечение		
П.1	1. AVAST Free Antivirus	Антивирусное ПО. Свободное, условно свободное

	2. AVG AntiVirus Free 3. Dr.Web Antivirus 4. Антивирус Касперского 5. ESET NOD32 Антивирус 6. AVZ Antivirus 7. Avira Free Antivirus 8. Norton AntiVirus 9. McAfee Antivirus 10. Emsisoft Anti-Malware 11. BullGuard Antivirus 12. Protector Plus Antivirus 13. Panda Antivirus 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus	или триал-версии.
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
П.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

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

6. Материально-техническое обеспечение дисциплины

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

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;

- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:

- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;

- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;

- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

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

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

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам дневной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 40	Неделя
Модуль 1 – 20 часа			
1	Характеристика защитных действий; Пресечение разглашения конфиденциальной информации;	2	1
2	«Исследование алгоритма симметричной системы шифрования данных – стандарт ГОСТ 28147-89».	2	2
3	«Изучение алгоритма открытого распределения ключей Диффи-Хелмана».	2	3
4	«Изучение алгоритма ассиметричной (двухключевой) системы шифрования данных RSA».	2	4
5	Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации.	2	5
6	Перечень сведений, отнесенных к государственной тайне. Указ президента российской федерации о перечне сведений, отнесенных к государственной тайне. 24 января 1998 года № 61. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера.	4	6
7	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 200 2 г. № 290.	2	7
8	Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами.	2	8
9	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	2	9
Модуль 2 – 20 часов			

10	Исследование характеристик и возможностей программ по организации резервного копирования Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности.	4	10
11	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	2	11
12	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	2	12
13	Анализ моделей нарушителя.	2	13
14	Угрозы информационно-программному обеспечению вычислительных систем и их классификация.	4	14
15	Основные способы защиты от потери информации и нарушений работоспособности сетей и систем.	2	15
16	Внесение функциональной и информационной избыточности; способы резервирования информации.	2	16
17	Правила обновления резервных данных.	2	17
18	Защита информации ограниченного доступа от утечки по техническим каналам	2	18

Студенты заочной формы обучения могут осваивать вопросы для самостоятельного изучения, представленные в подразделе 4.2 в произвольной последовательности, в удобное для них время. Однако к началу сессии они должны ориентироваться в материале курса.

Дополнения и изменения