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
_____ А.Г. Жуковский
«29» 08 2022 г.

Комплексное обеспечение защиты информации Б1.О.37
рабочая программа дисциплины

Кафедра: Общенаучной подготовки
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/7сем
Контактная работа, в том числе (по семестрам, курсам):		90/7сем
Лекции		40/7сем
Лабораторных работ		
Практических занятий		
Семинаров		50/7сем
Самостоятельная работа		90/7сем
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		1/7сем
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/7сем

Программу составил:
Профессор кафедры ИТСС, д.пол.н., к.т.н. доц. Жуковский А.Г.

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

Рабочая программа дисциплины
«Комплексное обеспечение защиты информации»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. №1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры ИТСС

Протокол от «29» 08 2022 г. № 1

Зав. кафедрой _____ В.Ю. 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 систем 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 систем 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 систем 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 систем связи»

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

1. Цели изучения дисциплины

Целью преподавания дисциплины «Комплексное обеспечение защиты информации» является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности компьютерных систем, а также содействие фундаментализации образования и развитию системного мышления.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями
Знать:
– принципы организации информационных систем в соответствии с требованиями по защите информации; – особенности комплексного подхода к обеспечению информационной безопасности организации;
Уметь:
– определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; – разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;
Владеть:
– владеть методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации; – владеть технологией разработки организационно-функциональной структуры и комплекса нормативно- методического обеспечения комплексной защиты информации на предприятии.
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
Знать:
– принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
Уметь:
– определять комплекс мер для обеспечения защиты информации объектов информатизации; – разработка предложений по совершенствованию системы управления защиты информации; – осуществлять планирование и организацию работы персонала, с учетом требований по

защите информации
Владеть:
– аналитикой информационной инфраструктуры информационной системы и ее безопасности объектов информатизации

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Комплексное обеспечение защиты информации» является логическим продолжением дисциплин Б1.О.11 «Основы информационной безопасности», Б1.В.01 «Введение в профессию», Б1.О.29 «Основы управления информационной безопасностью».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
2	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.39 «Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)», Б1.О.40 «Администрирование средств защиты информации в компьютерных системах и сетях»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 90 аудиторных часов, 90 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. (48+30) часов					
1.1	Лекция 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (вводная) 1. Основные концептуальные положения системы защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладению конфиденциальной информацией	Л1.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.2	Семинарское занятие 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВА 1. Основные положения государственной политики информационной безопасности 2. Ключевые проблемы информационной безопасности государства 3. Основные направления деятельности государства в области информационной безопасности	СЗ1.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.3	Лекция 2. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовое направление информационной безопасности 2. Организационное направление информационной безопасности 3. Инженерно-техническое направление информационной безопасности	Л2.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6

1.4	Семинарское занятие 2. ЗАКОНОДАТЕЛЬНАЯ, НОРМАТИВНО-МЕТОДИЧЕСКАЯ И НАУЧНАЯ БАЗА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ 1. Законодательство и промышленный шпионаж 2. Защита программного обеспечения авторским правом 3. Научно-методологический базис защиты информации 4. Стратегическая направленность защиты информации	СЗ2.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.5	Лекция 3. ОБЕСПЕЧЕНИЕ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ 1. Общие положения 2. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия 3. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну 4. Порядок работы с документами с грифом КТ 5. Обеспечение сохранности документов, дел и изданий. 6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну 7. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну 8. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну	Л3.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.6	Семинарское занятие 3. ИНФОРМАЦИОННАЯ СИСТЕМА КАК ОБЪЕКТ ЗАЩИТЫ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ 1. Разработка и производство информационных систем 2. Структура ИС и принципы ее функционирования 3. Проблемы защиты ИС 4. Системность подхода к защите информации 5. Трудности реализации СЗИ	СЗ3.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.7	Лекция 4. РАЗГЛАШЕНИЕ И УТЕЧКА ИНФОРМАЦИИ 1. Разглашение информации 2. Способы пресечения разглашения 3. Понятия утечки информации 4. Визуально-оптические каналы 5. Акустические каналы 6. Электромагнитные каналы 7. Материально-вещественные каналы утечки информации	Л4.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.8	Семинарское занятие 4. ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНЫХ УГРОЗ И КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ 1. Порядок отнесения информации к государственной тайне и распоряжение сведениями, составляющими государственную тайну 2. Угрозы информационной безопасности в сферах деятельности государства 3. Угрозы безопасности информации, ИС и субъектов информационных отношений 4. Угрозы для процессов, процедур и программ обработки информации 5. Угрозы информации, возникающие при побочных электромагнитных излучениях и наводках	СЗ4.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4

1.9	Лекция 5. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 1. Защита информации от утечки по визуально-оптическим каналам 2. Защита информации от утечки но акустическим каналам 3. Защита информации от утечки по электромагнитным каналам	Л5.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.10	Семинарское занятие 5. ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ОХРАННЫХ СИСТЕМ 1. Емкостные средства обнаружения нарушителей; 2. Допплеровские радиолучевые средства обнаружения; 3. Тепловизоры 4. Инфракрасные средства обнаружения нарушителей 5. Пьезоэлектрические датчики 6. Датчики, работающие на «эффекте Холла» 7. Ультразвуковые датчики 8. Системы электрического наведенного поля	С5.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.11	Лекция 6. 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	Л6.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.12	Семинарское занятие 6. ЗАЩИТА КАНАЛОВ СВЯЗИ 1. Криптографические методы и средства защиты информации 2. Защита данных при передаче по каналам связи ИС 3. Выбор и совместимость средств защиты сообщений 4. Брандмауэры - основа СЗИ 5. Технологии виртуальной частной сети для корпоративных пользователей	СЗ6.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.13	Лекция 7. ПРОТИВОДЕЙСТВИЕ РАДИОСИСТЕМАМ АКУСТИЧЕСКОГО ПОДСЛУШИВАНИЯ 1. Способы прослушивания посредством радиозакладок 2. Обеспечение безопасности телефонных переговоров 3. Противодействие лазерному прослушиванию	Л7.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.14	Семинарское занятие 7. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ НА ОБЪЕКТАХ ИС 1. Поиск радиозакладок с помощью носимых многофункциональных поисковых приборов. 2. Общая методология поиска радиозакладок 3. Поиск радиозакладок с помощью программно-аппаратных комплексов 4. Поиск возможных каналов утечки речевой информации за счет акустического воздействия на аппаратуру связи, оргтехнику и другие устройства 5. Методы выявления закладных устройств, подключаемых к телефонным и другим проводным линиям	С7.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.15	Лекция 8. ТРЕБОВАНИЯ К ЗАЩИТЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 1.Классификация требований к системам защиты информации. 2. Формализованные требования к защите информации от НСД. 3. Общие подходы к построению систем защиты компьютерной информации	Л8	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.16	Семинарское занятие 8. ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА	СЗ8.	4	ОПК-1.4;	Л1.1 Л1.2

	ЗАЩИТЫ ИНФОРМАЦИИ 1. Службы и механизмы защиты информации программно-техническими методами 2. Методы идентификации и аутентификации пользователей 3. Общие определения и классификация схем цифровых подписей 4. Инструментальные средства тестирования системы защиты 5. Межсетевые экраны 6. Виртуальные частные сети и их информационная защита			ОПК-10	Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
1.17	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ. Федеральный закон "О связи" от 07.07.2003 №126-ФЗ. Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ. Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ. Закон РФ "О государственной тайне" от 21.07.1993 №5485-1. Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 №40-ФЗ	СРС	30	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
	Модуль 2. (42+30) часов				
2.1	Лекция 9. СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ 1. Основные понятия 2. Перечень продукции, процессов и услуг, подлежащих сертификации 3. Процесс сертификации 4. Порядок подготовки и проведения сертификации 5. Типовой алгоритм испытаний ПО на соответствие требованиям безопасности	Л9.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.2	Семинарское занятие 9 ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ 1. Организация документооборота на предприятии 2. Организация службы безопасности на предприятии. 3. Состав службы безопасности на предприятии. 4. Организация охранного видеонаблюдения 5. Организация защиты информации в ИС от утечки по каналам ПЭМИН 6. Процесс сертификации ИС и программного обеспечения на соответствие требованиям безопасности	С9.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.3	Лекция 10. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Принципы политики безопасности 2. Виды политики безопасности 3. Организационно-технические мероприятия политики информационной безопасности 4. Основные требования политики информационной безопасности. 5. Уровни политики безопасности 6. Роли и обязанности должностных лиц в соблюдении политики безопасности	Л10.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.4	Семинарское занятие 10. ПРОБЛЕМЫ БЕЗОПАСНОСТИ В СЕТИ INTERNET 1. Internet в структуре информационно-аналитического обеспечения органов государственной власти 2. Угрозы для протоколов и служб Internet 3. Потенциальные проблемы с электронной почтой 4. Обеспечение конфиденциальности сообщений и данных.	С310.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1

	Обеспечение целостности данных и сообщений				Л2.2 Л2.3 Л2.4
2.5	Лекция 11. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (Продолжение лекции 9)	Л11.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.6	Семинарское занятие 11 ЗАЩИТА ПРОЦЕССОВ И ПРОГРАММ 1. Проблемы безопасности программного обеспечения 2. Механизмы защиты процессов, процедур и программ обработки данных 3. Защита процессов и процедур передачи информации по каналам связи ИС 4. Принципы использования цифровой подписи для защиты электронных документов 5. Защита операционных систем	С11.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.7	Лекция 12. ПОНЯТИЯ ТЕОРИИ НАДЕЖНОСТИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Оценка надежности систем защиты информации 2. Задача и методы резервирования встроенных в ОС механизмов защиты для повышения отказоустойчивости системы защиты	Л12.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.8	Семинарское занятие 12. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕТЕЙ ОБЩЕГО ПОЛЬЗОВАНИЯ 1. Проблемы использования Internet в структуре информационно-аналитического обеспечения органов государственной власти 2. Политика информационной безопасности для WEB-сервера 3. Возможности нарушений информационной безопасности при использовании стека протоколов TCP/IP 4. Возможности нарушений информационной безопасности при использовании сервисов Интернет 5. Сложность конфигурирования и мер защиты при использовании сетей общего пользования. 6. Угрозы информационной безопасности при использовании беспроводных сетей.	СЗ12.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.9	Лекция 13. АНАЛИЗ ЗАЩИЩЕННОСТИ СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ 1. Основные защитные механизмы ОС семейства UNIX 2. Принципиальные недостатки защитных механизмов ОС семейства UNIX 3. Основные защитные механизмы ОС семейства Windows 4. Принципиальные недостатки защитных механизмов ОС семейства Windows 5. Особенности защитных механизмов macOS	Л13.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.10	Семинарское занятие 13. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ 1. Принципы организации и контроля системы защиты 2. Мониторинг функционирования ИС 3. Управление защитой в распределенных сетях 4. Методы разработки защищенных ИС 5. Функции контроля и управление СЗИ 6. Построение системы защиты информации 7. Порядок проведения работ по ЗИ	СЗ13.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.11	Лекция 14. ОЦЕНКА УЯЗВИМОСТИ И РИСКОВ 1. Процесс анализа рисков 2. Элементы управления рисками	Л14.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4

	3. Этапы процесса управления рисками 4. Методики оценки потенциально возможных угроз ИС				Л1.5 Л1.6
2.12	Семинарское занятие 14. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ. 1. Вероятностный подход: структуризация предметной области оценки, анализ. 2. Подход на основе формирования требований к объекту: классы защищенности и их характеристики, контрольные процедуры, определение соответствия защиты установленным требованиям 3. Содержание и особенности экспертной оценки эффективности защиты. 4. Классификационная структура методов и моделей оценки 5. Системы показателей защищенности (эффективности). 6. Области применения и анализ приемлемости различных методов и моделей для оценки эффективности	СЗ14.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.13	Лекция 15. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИСО 19011:2011) 1. Разработка программы аудита. Проведение аудита. Компетентность и оценка аудиторов. Формирование выводов аудита 2. Сфера действия, политика и подход к оценке риска системы менеджмента информационной безопасности (СМИБ) организации 3. Идентификация, анализ и оценивание риска, идентификация и оценивание вариантов обработки риска 4. Реализация, функционирование и мониторинг СМИБ 5. Совершенствование СМИБ	Л15.	2	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.14	Семинарское занятие 15. СТРУКТУРА И ЗАДАЧИ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ЗАЩИТУ ИНФОРМАЦИИ 1. Назначение, состав и функции службы защиты информации предприятия. 2. Механизмы создания службы защиты информации. 3. Правовой статус службы защиты информации. 4. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций службы защиты информации. 5. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ. 6. Функции сотрудников и уполномоченных службы защиты информации. 7. Организация взаимодействия службы защиты информации и подразделений предприятия и внешних организаций.	СЗ15.	4	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.15	Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11.03.1992 №2487-1 Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ. Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ . Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности	СРС	30	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4

3.1	**Курсовая работа**	СРС	30	ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
	Экзамен			ОПК-1.4; ОПК-10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
Итого – 180 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	Семенов, Ю. А.	Процедуры, диагностики и безопасность в Интернет: учебное пособие / Ю. А. Семенов	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с.	Э1
Л1.2	Беленькая, М. Н.	Администрирование в информационных системах: учебное пособие для вузов / М. Н. Беленькая, С. Т. Малиновский, Н. В. Яковенко.	Москва : Горячая линия-Телеком, 2018. - 408 с.	Э2
Л1.3	Белов, Е. Б.	Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др.	Москва : Гор. линия-Телеком, 2011. - 558 с.	Э3
Л1.4	Курило А.П., Милославская Н.Г., Сенаторов М.Ю.	Вопросы управления информационной безопасностью: Учебное пособие для вузов.	Москва :Гор. линия-Телеком, 2013. - 244 с.	Э4
Л1.5	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов	Москва :Гор. линия-Телеком, 2013. - 214 с.	Э5
Л1.6	Бузов, Г. А.	Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие	Москва :Гор. линия-Телеком, 2015. - 586 с.	Э6

5.1.2. Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	В.А. Ворона, В.А. Тихонов.	Инженерно-техническая и пожарная защита объектов	Москва : Гор. линия-Телеком, 2012. - 512 с.	Э7

Л2.2	Бузов, Г. А.	Практическое руководство по выявлению специальных технических средств несанкционированного получения информации	Москва : Гор. линия-Телеком, 2013. - 240 с.	Э8
Л2.3	Завгородний В.И.	Комплексная защита информации в компьютерных системах: Учебное пособие.	М.: Логос, 2001. - 264 с : ил.	2
Л2.4	Ярочкин В.И.	Информационная безопасность: Учебник для студентов вузов.	М.: Академический Проект; 2-е изд.— 2004. — 544 с.	10

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.

5.2. Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/120489.html
Э2	https://znanium.com/catalog/document?id=365184
Э3	https://znanium.com/catalog/document?id=233208
Э4	https://znanium.com/catalog/document?id=14942
Э5	https://znanium.com/catalog/document?id=241916
Э6	https://znanium.com/catalog/document?id=45737
Э7	https://znanium.com/catalog/document?id=178536
Э8	https://znanium.com/catalog/document?id=253276

5.3. Программное обеспечение

П.1	MS Word	лицензионное
П.2	Power Point	лицензионное

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 с пакетом офисных программ и выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория с пакетом офисных программ и выходом в интернет

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 очной 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: 72	Неделя
Модуль 1 – 30 часов			
1	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ.	4	1
2	Федеральный закон "О связи" от 07.07.2003 №126-ФЗ.	4	2
3	Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ	4	3
4	Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ.	4	4
5	Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ.	4	5
6	Закон РФ "О государственной тайне" от 21.07.1993 №5485-1.	4	6
7	Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ.	3	7
8	Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 №40-ФЗ	3	8
Модуль 2 – 30 часов			
9	Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11.03.1992 №2487-1	4	9
10	Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ.	4	10
11	Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ .	4	11
12	Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ.	4	12
13	Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ.	4	13
14	Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ.	4	14
15	"Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ.	3	15
16	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности	3	16

Дополнения и изменения в рабочей программе