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
«29» 04 2024 г.

Комплексное обеспечение защиты информации объекта информатизации Б1.О.33

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	6	216/8 сем
Контактная работа, в том числе (по семестрам, курсам):		96/8 сем
Лекции		36/8 сем
Лабораторных работ		24/8 сем
Практических занятий		36/8 сем
Семинаров		
Самостоятельная работа		84/8 сем
Контроль		36/8 сем
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		1/8 сем
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/8 сем

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

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

Рабочая программа дисциплины
«Комплексное обеспечение защиты информации объекта информатизации»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

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

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

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

"Информационная безопасность"

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
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины **" Комплексное обеспечение защиты информации объекта информатизации "** 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 ***организационно-управленческой деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
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:
- угрозы информационной безопасности, меры защиты и противодействия; - принципы разработки политики безопасности; - основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты, требования и рекомендации по защите информации и требования по технической защите информации; - принципы управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации
Уметь:
- строить концептуальные модели информационной безопасности объекта защиты; - разрабатывать политики безопасности с учетом угроз безопасности информации и требований по защите информации; - использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; - разрабатывать организационные и технические мероприятия управления доступом и информационными потоками в компьютерных системах с учетом особенностей конкретного предприятия
Владеть:
- навыками выявления угроз информационной безопасности на объекте защиты; - навыками разработки, правильного оформления, презентации и внедрения разрабатываемых политик безопасности; - навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима; - навыками проведения организационных и технических мероприятий по управлению доступом и информационными потоками в компьютерных системах.
ПК-2: способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
Знать:
- виды политик безопасности компьютерных систем и сетей; - модели безопасности компьютерных систем;

- организационные меры по обеспечению информационной безопасности объекта защиты
Уметь:
- анализировать объект защиты информации с целью определения необходимого уровня защищенности и доверия; - формулировать задания по обеспечению информационной безопасности объекта защиты.
Владеть:
- навыками формирования политики безопасности компьютерных систем и сетей; - навыками разработки профилей защиты компьютерных систем.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.27 Основы информационной безопасности
2	Б1.О.28 Организационное и правовое обеспечение информационной безопасности
3	Б1.О.32 Основы управления информационной безопасностью
4	Б1.О.30 Программно-аппаратные средства защиты информации
5	Б1.О.31 Защита информации от утечки по техническим каналам
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.01 Обеспечение безопасности персональных данных в информационных системах
2	Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 216 часов, 96 аудиторных часов, 84 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 8					
Модуль 1.					
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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.2	Практическое 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	ПЗ1.	4	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5

					Л1.6
1.4	Практическое 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	ПЗ2.	4	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.6	Практическое 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	ПЗ3.	4	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.8	Лабораторная работа 1. 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	ЛР1	4	ОПК-10 ПК-2	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.	4	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.10	Практическое занятие 4. ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ	ПЗ4.	4	ОПК-10	Л1.1

	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			ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.12	Лабораторная работа 2. 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	ЛР2	4	ОПК-10 ПК-2	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.	4	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.14	Лабораторная работа 3. 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	ЛР3	4	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
1.16	Практическое занятие 5. ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА 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	ПЗ5.	4	ОПК-10 ПК-2	Л1.1 Л1.2 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.	СРС	26	ОПК-10	Л1.1 Л1.2

	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			ПК-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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.2	Практическое занятие 6 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	ПЗ6.	4	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.4	Лабораторная работа 4. 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. Обеспечение целостности данных и сообщений	ЛР4.	4	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л2.4
2.5	Лекция 11. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (Продолжение лекции 9)	Л11.	2	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.6	Лабораторная работа 5 ЗАЩИТА ПРОЦЕССОВ И ПРОГРАММ 1. Проблемы безопасности программного обеспечения 2. Механизмы защиты процессов, процедур и программ обработки данных	ЛР5.	4	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5

	3. Защита процессов и процедур передачи информации по каналам связи ИС 4. Принципы использования цифровой подписи для защиты электронных документов 5. Защита операционных систем				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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.8	Лабораторная работа 6. 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.	ЛР6.	4	ОПК-10 ПК-2	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.	4	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.10	Практическое занятие 7. 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	ПЗ7.	4	ОПК-10 ПК-2	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 3. Этапы процесса управления рисками 4. Методики оценки потенциально возможных угроз ИС	Л14.	2	ОПК-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.12	Практическое занятие 8. 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	ПЗ8.	4	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
2.14	Практическое занятие 9. 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.	ПЗ9.	4	ОПК-10 ПК-2	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	28	ОПК-10 ПК-2	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-10 ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6
	Экзамен		36		
Итого – 216 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.	Москва: Интернет-Университет Инфор-	Э1

		Семенов	мационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с.	
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

5.2. 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	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Kaspersky Endpoint Security (лицензия)

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	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из

виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к экзамену осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к экзамену необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к экзамену, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе