

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 УР

Н.А. Андреева

« 08 » « 09 » 2026 г.

Рабочая программа дисциплины

**Б1.В.02 Комплексное обеспечение защиты информации объекта
информатизации**

Кафедра: Информационная безопасность
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	ОФ	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	6	216/8
Контактная работа, в том числе (по семестрам, курсам):		96/8
Лекции		48/8
Лабораторных работ		
Практических занятий		48/8
Семинаров		
Самостоятельная работа		84/8
Контроль		36/8
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		1/8
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/8

Программу составил:
Профессор кафедры ИБ, д.пол.н., к.т.н. доцент Жуковский А.Г.

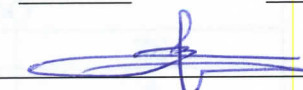
Рабочая программа дисциплины
«Комплексное обеспечение защиты информации объекта информатизации»

Разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования 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 № 8 от 31.03. 2026 г., и утвержденного директором СКФ МТУСИ 31.03. 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационная безопасность

Протокол от «28» 04 2026. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания 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 обучающихся способности решать профессиональные задачи в соответствии с **эксплуатационным** видом деятельности.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ПК-1: Администрирование подсистем защиты информации в операционных системах
Знать: архитектуру и принципы построения операционных систем; программные интерфейсы операционных систем; виды политик управления доступом; архитектуру подсистем защиты информации в операционных системах; состав типовых конфигураций программно-аппаратных средств защиты информации; методы и средства антивирусной защиты в операционных системах; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации
Уметь: формировать политики безопасности операционных систем; оценивать угрозы безопасности информации операционных систем; противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем; настраивать антивирусные средства защиты информации в операционных системах; устанавливать обновления программного обеспечения и средств антивирусной защиты; оценивать угрозы безопасности информации в операционных системах; обосновывать выбор используемых программно-аппаратных средств защиты информации в операционных системах ограниченного доступа в организации;
Владеть: навыками определения состава применяемых программно-аппаратных средств защиты информации в операционных системах; навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации; управлением антивирусной защитой операционных систем в соответствии с действующими требованиями; программно-аппаратными средствами и методами защиты информации в операционных системах; нормативными правовыми актами в области защиты информации.
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
Знать: программные средства системного и прикладного назначения, в том числе отечественного

производства, и принципы их применения при решении задач профессиональной деятельности;
 методы и средства обеспечения информационной безопасности в компьютерных сетях;
 нормативно-правовые акты, регулирующие защиту информации;
 алгоритмы и протоколы шифрования данных;
 принципы администрирования сетевых экранов (файрволов);
 методы мониторинга и анализа событий в компьютерных сетях для выявления потенциальных угроз;
 инструменты и методы управления доступом к информационным ресурсам;
 технологии аутентификации и авторизации пользователей в сети;
 способы обеспечения целостности и доступности информации;
 принципы функционирования сетевых протоколов, включающих криптографические алгоритмы.

Уметь:

настраивать и управлять программными и аппаратными средствами защиты информации в компьютерных сетях;
 устанавливать и обновлять антивирусное программное обеспечение; настраивать файрволы и другие сетевые экраны для защиты от внешних угроз;
 настраивать протоколы шифрования данных;
 управлять политиками безопасности в сетевых операционных системах; реагировать на инциденты безопасности и принимать меры по устранению последствий;
 настраивать системы обнаружения и предотвращения вторжений (IDS/IPS);
 оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях

Владеть:

навыками настройки и управления программных и аппаратных средств защиты информации в компьютерных сетях;
 методами мониторинга и анализа событий безопасности в компьютерных сетях;
 технологиями установки и настройки межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS);
 способами настройки антивирусного программного обеспечения и систем защиты от вредоносного ПО;
 методами управления учётными записями, правами доступа и политиками безопасности;
 навыками внедрения и настройки систем шифрования данных; навыками конфигурирования защищенного удаленного доступа;
 навыками конфигурирования аппаратно-программных средств для организации виртуальных частных сетей.

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.27 «Основы информационной безопасности», Б1.В.06 «Введение в профессию», Б1.О.32 «Основы управления информационной безопасностью».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
2	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.36.06 «Администрирование средств защиты информации в компьютерных системах и сетях», Б1.О.30 «Моделирование систем защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 216 часов, 96 аудиторных часов (48 лекций и 48 практики, 84 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 8					
Модуль 1.					
24 часов лекций, 24 часа практики, 42 часа самостоят работа					
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	Лек1.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
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	ПЗ 1.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
1.3	Лекция 2. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовое направление информационной безопасности 2. Организационное направление информационной безопасности 3. Инженерно-техническое направление информационной безопасности	Лек2.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
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	ПЗ 2.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	Лек3.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4

	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				
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	ПЗ 3.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	Лек4.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
1.8	Практическое 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	ПЗ 4.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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 по акустическим каналам 3. Защита информации от утечки по электромагнитным	Лек5.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4

	каналам				
1.10	Практическое 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	ПЗ 5.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	Лек6.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
1.12	Практическое 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	ПЗ 6.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
1.13	Лекция 7. ПРОТИВОДЕЙСТВИЕ РАДИОСИСТЕМАМ АКУСТИЧЕСКОГО ПОДСЛУШИВАНИЯ 1. Способы прослушивания посредством радиозакладок 2. Обеспечение безопасности телефонных переговоров 3. Противодействие лазерному прослушиванию	Лек7.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
1.14	Практическое 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	ПЗ 7.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2

	линиям				
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	Лек8	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
1.16	Практическое занятие 8. 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	ПЗ 8.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	42	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
Модуль 2. 24 часов лекций, 24 часа практики, 42 часа самостоятельная работа					
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	Лек9.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4

	5. Типовой алгоритм испытаний ПО на соответствие требованиям безопасности				
2.2	Практическое 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	ПЗ 9.	4	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	Лек10.	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
2.4	Практическое 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. Обеспечение целостности данных и сообщений	ПЗ 10	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
2.5	Лекция 11. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (Продолжение лекции 9)	Лек11.	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
2.6	Практическое 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	ПЗ 11	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
2.7	Лекция 12. ПОНЯТИЯ ТЕОРИИ НАДЕЖНОСТИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Лек12.	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3

	1. Оценка надежности систем защиты информации 2. Задача и методы резервирования встроенных в ОС механизмов защиты для повышения отказоустойчивости системы защиты				Л1.4
2.8	Практическое 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.	ПЗ 12	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	Лек13.	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
2.10	Практическое 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	ПЗ 13	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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	Лек14.	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
2.12	Практическое занятие 14. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ. 1. Вероятностный подход: структуризация предметной области оценки, анализ.	ПЗ 14	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1

	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				Л2.2
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	Лек15.	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
2.14	Практическое 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.	ПЗ 15	2	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2
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 .	СРС	22	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2

	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				
3.1	Курсовая работа	CPC	20	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4
	Экзамен		36	ПК-1; ПК-2	Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л2.2 Л3.1 Л3.2
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	Э. В. Запонов, А. П. Мартынов, И. Г. Машин	Методы и средства комплексной защиты информации в технических системах : учебное пособие	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2019	Э1
Л1.2	Бузов, Г. А.	Защита информации ограниченного доступа от утечки по техническим каналам: Учебное пособие	Москва :Горячая линия-Телеком, 2024. – 585 с.	Э2
Л1.3	Штеренберг, С. И.	Защита информации в компьютерных системах : учебное пособие	Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2022.	Э3
Л1.4	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов : Профобразование, 2024. — 702 с.	Э4
5.1.2. Дополнительная литература				

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Шаньгин, В. Ф.	Комплексная защита информации в корпоративных системах : учебное пособие	Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с.	Э5
Л2.2	Литвинов, Р.В., К.А. Волегов, А.П. Бацула	Технические средства защиты информации. Часть 1 : курс лекций	Томск : Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с.	Э6
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Компания «Конфидент»	Защита информации. Dallas Lock : практикум / видеоуроки	База знаний Dallas Lock	Э7
Л3.2	ФСТЭК	Официальный сайт ФСТЭК РФ. Раздел «Документы»	2025. Федеральная служба по техническому и экспортному контролю	Э8
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/101925.html			
Э2	https://elib.mtuci.ru/view.php?book_id=3168			
Э3	https://www.iprbookshop.ru/140114.html			
Э4	https://www.iprbookshop.ru/145912.html			
Э5	https://znanium.ru/catalog/product/1843022			
Э6	https://www.iprbookshop.ru/14027.html			
Э7	https://dallaslock.ru/products/faq/			
Э8	https://fstec.ru/dokumenty-filter			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Электронный ресурс http://www.securitylab.ru/			
5.3.5	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.6	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.7	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	MS Word	Лицензионное ПО		
П.2	Power Point	Лицензионное ПО		
П.3	Kaspersky Endpoint Security	Лицензионное ПО		
П.4	Операционная система Linux	Свободное ПО		

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором, ПК (ноутбуком), экраном
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.
--

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на

соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.В.02 Комплексное обеспечение защиты информации объекта информатизации» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____

(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не

		может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	--

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ПК-1: Администрирование подсистем защиты информации в операционных системах		
Знать:		
архитектуру и принципы построения операционных систем; программные интерфейсы операционных систем; виды политик управления доступом; архитектуру подсистем защиты информации в операционных системах; состав типовых конфигураций программно-аппаратных средств защиты информации; методы и средства антивирусной защиты в операционных системах; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации	Контрольная работа 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-8 «Отлично» - 9-10
	Контрольная работа 2	Модуль 2 0÷15 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-7 «Хорошо» - 8-11 «Отлично» - 12-15
Уметь:		
формировать политики безопасности операционных систем; оценивать угрозы безопасности информации операционных систем; противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем; настраивать антивирусные средства защиты информации в операционных системах; устанавливать обновления программного обеспечения и средств антивирусной защиты; оценивать угрозы безопасности информации в операционных системах; обосновывать выбор используемых программно-аппаратных средств защиты информации в операционных	Практические занятия 1-8	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практические занятия 9-15	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5

системах ограниченного доступа в организации		
Владеть:		
навыками определения состава применяемых программно-аппаратных средств защиты информации в операционных системах; навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации; управлением антивирусной защитой операционных систем в соответствии с действующими требованиями; программно-аппаратными средствами и методами защиты информации в операционных системах; нормативными правовыми актами в области защиты информации	Практические занятия 1-8	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практические занятия 9-15	Модуль 2 0÷10 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях		
Знать:		
программные средства системного и прикладного назначения, в том числе отечественного производства, и принципы их применения при решении задач профессиональной деятельности; методы и средства обеспечения информационной безопасности в компьютерных сетях; нормативно-правовые акты, регулирующие защиту информации; алгоритмы и протоколы шифрования данных; принципы администрирования сетевых экранов (файрволов); методы мониторинга и анализа событий в компьютерных сетях для выявления потенциальных угроз; инструменты и методы управления доступом к информационным ресурсам; технологии аутентификации и авторизации пользователей в сети; способы обеспечения целостности и доступности информации; принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	Контрольная работа 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-8 «Отлично» - 9-10
	Контрольная работа 2	Модуль 2 0÷15 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-7 «Хорошо» - 8-11 «Отлично» - 12-15
Уметь:		
настраивать и управлять программными и аппаратными средствами защиты информации в компьютерных сетях;	Практические занятия 1-8	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3
устанавливать и обновлять антивирусное		

программное обеспечение; настраивать фаерволы и другие сетевые экраны для защиты от внешних угроз; настраивать протоколы шифрования данных; управлять политиками безопасности в сетевых операционных системах; реагировать на инциденты безопасности и принимать меры по устранению последствий; настраивать системы обнаружения и предотвращения вторжений (IDS/IPS); оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях		«Хорошо» - 4 «Отлично» - 5
	Практические занятия 9-15	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Владеть:		
навыками настройки и управления программных и аппаратных средств защиты информации в компьютерных сетях; методами мониторинга и анализа событий безопасности в компьютерных сетях; технологиями установки и настройки межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS); способами настройки антивирусного программного обеспечения и систем защиты от вредоносного ПО; методами управления учётными записями, правами доступа и политиками безопасности; навыками внедрения и настройки систем шифрования данных; навыками конфигурирования защищенного удаленного доступа; навыками конфигурирования аппаратно-программных средств для организации виртуальных частных сетей	Практические занятия 1-8	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практические занятия 9-15	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Экзамен	0-100 баллов: «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы для текущего контроля и промежуточной аттестации: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства текущего контроля для очной формы обучения

Данная дисциплина формирует у обучающегося 2 компетенции, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе обучающегося на контрольный вопрос или при выполнении практического или лабораторного

задания достаточно сложно. Предлагается считать, что вклад 2-х компетенций в общую оценку при ответе на вопрос примерно одинаков.

Модуль 1 (50 баллов):

Модуль содержит 8 лекционных занятий и 8 семинарских работ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За семинарские занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ПК-1; ПК-2):

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией
5. Правовое направление информационной безопасности
6. Организационное направление информационной безопасности
7. Инженерно-техническое направление информационной безопасности
8. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия
9. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну
10. Порядок работы с документами с грифом КТ
11. Обеспечение сохранности документов, дел и изданий.
12. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну
13. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну
14. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну
15. Способы разглашения информации
16. Способы пресечения разглашения
17. Понятия утечки информации
18. Визуально-оптические каналы
19. Акустические каналы
20. Электромагнитные каналы
21. Материально-вещественные каналы утечки информации
22. Защита информации от утечки по визуально-оптическим каналам
23. Защита информации от утечки по акустическим каналам
24. Защита информации от утечки по электромагнитным каналам
25. Способы несанкционированного доступа
26. Технические средства несанкционированного доступа к информации
27. Защита от наблюдения и фотографирования
28. Защита от подслушивания
29. Способы прослушивания посредством радиозакладок
30. Обеспечение безопасности телефонных переговоров
31. Противодействие лазерному прослушиванию
32. Классификация требований к системам защиты информации.
33. Формализованные требования к защите информации от НСД.
34. Общие подходы к построению систем защиты компьютерной информации

Практическое занятие 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВА (ПК-1; ПК-2):

1. Основные положения государственной политики информационной безопасности
2. Ключевые проблемы информационной безопасности государства
3. Основные направления деятельности государства в области информационной безопасности

Практическое занятие 2. ЗАКОНОДАТЕЛЬНАЯ, НОРМАТИВНО-МЕТОДИЧЕСКАЯ И НАУЧНАЯ БАЗА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ (ПК-1; ПК-2):

1. Законодательство и промышленный шпионаж
2. Защита программного обеспечения авторским правом
3. Научно-методологический базис защиты информации
4. Стратегическая направленность защиты информации

Практическое занятие 3. ИНФОРМАЦИОННАЯ СИСТЕМА КАК ОБЪЕКТ ЗАЩИТЫ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ (ПК-1; ПК-2):

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

Практическое занятие 4. ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНЫХ УГРОЗ И КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ (ПК-1; ПК-2):

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

Практическое занятие 5. . ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ОХРАННЫХ СИСТЕМ (ПК-1; ПК-2):

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

Практическое занятие 6. ЗАЩИТА КАНАЛОВ СВЯЗИ (ПК-1; ПК-2):

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

Практическое занятие 7. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ НА ОБЪЕКТАХ ИС (ПК-1; ПК-2):

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

Практическое занятие 8. ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ (ПК-1; ПК-2):

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

Модуль 2: (50 баллов):

Модуль содержит 7 лекционных и 7 семинарских занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За семинарские занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 2 (ПК-1; ПК-2):

1. Перечень продукции, процессов и услуг, подлежащих сертификации
2. Процесс сертификации
3. Порядок подготовки и проведения сертификации
4. Типовой алгоритм испытаний ПО на соответствие требованиям безопасности
5. Принципы политики безопасности
6. Виды политики безопасности
7. Организационно-технические мероприятия политики информационной безопасности
8. Основные требования политики информационной безопасности.
9. Уровни политики безопасности
10. Роли и обязанности должностных лиц в соблюдении политики безопасности
11. Оценка надежности систем защиты информации
12. Задача и методы резервирования встроенных в ОС механизмов защиты для повышения отказоустойчивости системы защиты
12. Основные защитные механизмы ОС семейства UNIX
14. Принципиальные недостатки защитных механизмов ОС семейства UNIX
15. Основные защитные механизмы ОС семейства Windows
16. Принципиальные недостатки защитных механизмов ОС семейства Windows
17. Особенности защитных механизмов macOS
18. Процесс анализа рисков
19. Элементы управления рисками
20. Этапы процесса управления рисками
21. Методики оценки потенциально возможных угроз ИС

22. Разработка программы аудита. Проведение аудита. Компетентность и оценка аудиторов. Формирование выводов аудита
23. Сфера действия, политика и подход к оценке риска системы менеджмента информационной безопасности (СМИБ) организации
24. Идентификация, анализ и оценивание риска, идентификация и оценивание вариантов обработки риска
25. Реализация, функционирование и мониторинг СМИБ
26. Совершенствование СМИБ

Практическое занятие 9. ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ (ПК-1; ПК-2):

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

Практическое занятие 10. ПРОБЛЕМЫ БЕЗОПАСНОСТИ В СЕТИ INTERNET (ПК-1; ПК-2):

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

Практическое занятие 11. ЗАЩИТА ПРОЦЕССОВ И ПРОГРАММ (ПК-1; ПК-2):

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

Практическое занятие 12. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕТЕЙ ОБЩЕГО ПОЛЬЗОВАНИЯ (ПК-1; ПК-2):

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.

Практическое занятие 13. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ (ПК-1; ПК-2):

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

Практическое занятие 14. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ (ПК-1; ПК-2):

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

Практическое занятие 15. СТРУКТУРА И ЗАДАЧИ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ЗАЩИТУ ИНФОРМАЦИИ (ПК-1; ПК-2):

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.

1.3.2 Модуль «Курсовая работа» (100 баллов):

Тема курсовой работы:

1. Разработка комплексной системы информационной безопасности на предприятии (по отдельному методическому руководству).

Для выполнения курсовой работы обучающиеся получают в библиотеке или скачивают с методического раздела сайта СКФ МТУСИ методическое пособие: Жуковский А.Г. **Комплексное обеспечение защиты информации:** Методические указания по выполнению курсовой работы.

Модуль посвящен выполнению задания на курсовую работу. Максимальное количество баллов за выполненную и защищенную курсовую работу составляет 100.

Курсовая работа выполняется в процессе освоения компетенций ПК-1 и ПК-2 и ее итоговая оценка характеризует заключительный этап их освоения. Ввиду сложности определения вклада той или иной компетенции в курсовую работу, для упрощения процедуры оценивания будем считать, что их вклад в курсовую работу одинаков, а максимальное количество баллов за каждую компетенцию может составить 50. Критерии оценки курсовой работы приведены в таблице 1.

Таблица 1 – Критерии оценки курсовой работы

№п/п	Оцениваемые параметры	Оценка в баллах
1.	Выполнение задания на курсовую работу: - Задание выполнено в полном объеме, каждый рассматриваемый вопрос раскрыт полностью, разработанная система соответствует предъявляемым к ней требованиям. - Задание выполнено в полном объеме, один или несколько рассматриваемых вопросов раскрыты неполно, разработанная система соответствуют предъявляемым к ней требованиям. - Один или несколько пунктов задания не выполнены или выполнены не в полном объеме	20 10 0
2.	Использование демонстрационного материала: - демонстрационный материал включает в себя технические требования к системе, расчеты, ряд иллюстраций, поясняющих расчеты. - демонстрационный материал включает в себя технические требования к системе, иллюстрации. - демонстрационный материал включает в себя иллюстрации. - демонстрационный материал не отражает основных этапов проектирования.	20 14 8 2
3.	Оформление результатов работы - курсовая работа оформлена в полном соответствии с ЕСКД; - курсовая работа оформлена с незначительными отклонениями от ЕСКД; - оформление курсовой работы не соответствует требованиям ЕСКД.	20 10 4
4.	Качество ответов на вопросы: - отвечает на вопросы; - не может ответить на большинство вопросов; - не может четко ответить на вопросы.	40 24 13

Обучающийся, набравший от 41 до 60 баллов, получает оценку «удовлетворительно», от 61 до 80 баллов, получает оценку «хорошо», от 81 до 100 баллов – оценку «отлично». Обучающийся получает оценку «неудовлетворительно» если набрал от 0 до 40 баллов.

1.3.3 Вопросы, выносимые на экзамен по дисциплине «Комплексное обеспечение защиты информации объекта информатизации» (ПК-1; ПК-2) (промежуточная аттестация)

1. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ.
2. КСЗИ как сложная человеко-машинная система. Основные положения теории систем.
3. Принципы организации КСЗИ. Основные требования, предъявляемые к КСЗИ.
4. Состав и содержательная характеристика этапов разработки КСЗИ.
5. Основные факторы, влияющие на организацию КСЗИ.
6. Характер и степень влияния различных факторов на организацию КСЗИ.
7. Методика определения состава защищаемой информации. Этапы работы по выявлению состава защищаемой информации.
8. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации.
9. Классификация информации по видам тайны и степеням конфиденциальности. Нормативное закрепление состава защищаемой информации; структура перечней сведений,

относимых к различным видам тайны.

10. Особенности помещений для работы с защищаемой информацией как объектов защиты.

11. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.

12. Состав средств обеспечения функционирования предприятия, подлежащих защите.

13. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия. Методика выявления способов воздействия на информацию.

14. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

15. Методика выявления каналов несанкционированного доступа к информации.

16. Определение возможных методов несанкционированного доступа к защищаемой информации.

17. Оценка степени опасности применения различных методов. Анализ потенциальных последствий реализации несанкционированного доступа.

18. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.

19. Определение направлений и возможностей доступа нарушителей к защищаемой информации.

20. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.

21. Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ.

22. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования КСЗИ.

23. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество защиты.

24. Понятие модели объекта, основные виды моделей и их характеристика.

25. Модель как инструмент количественного и качественного анализа КСЗИ. Значение моделирования процессов КСЗИ.

26. Выбор структуры КСЗИ, ее зависимость от объектов защиты, характера и условий функционирования предприятия.

27. Функциональная модель КСЗИ. Организационная модель КСЗИ. Информационная модель КСЗИ.

28. Общее содержание работ по организации КСЗИ. Характеристика основных стадий создания КСЗИ.

29. Определение состава кадрового обеспечения функционирования КСЗИ. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.

30. Перечень нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.

31. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ.

32. Значение нормативно-методического обеспечения функционирования КСЗИ. Перечень вопросов, требующих документационного закрепления.

33. Понятие и виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ. Методы контроля.

34. Особенности проведения контроля функционирования КСЗИ. Анализ и использование результатов проведения контрольных мероприятий.

35. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации.
36. Классификация подходов к оценке эффективности систем защиты информации. Вероятностный подход.
37. Классификация подходов к оценке эффективности систем защиты информации. Оценочный подход на основе формирования требований к защищенности объекта.
38. Содержание и особенности экспертной оценки эффективности защиты.
39. Классификационная структура методов и моделей оценки информационной защищенности. Базовые понятия и определения, используемые в моделях.
40. Системы показателей защищенности (эффективности). Метод оценки уровня безопасности и аналитические модели определения базовых и обобщенных показателей уязвимости.
41. Основные понятия теории надежности. Понятие резервирования, виды резервирования.
42. Рекомендации по разработке охранно-пропускного режима на предприятии
43. Сведения, составляющие коммерческую тайну предприятия
44. Обязанности лиц, допущенных к сведениям, содержащим конфиденциальную информацию.
45. Порядок ведения делопроизводства документов, содержащих коммерческую тайну
46. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну
47. Угрозы для протоколов и служб Internet
48. Виртуальные частные сети и их информационная защита
49. Методы идентификации и аутентификации пользователей
50. Инструментальные средства тестирования системы защиты
51. Межсетевые экраны
52. Оценка защищенности информации от утечки по каналам ПЭМИН
53. Управление защитой в распределенных сетях
54. Аудит информационной безопасности
55. Методика аудита выделенных помещений
56. Действия, приводящие к неправомерному овладению конфиденциальной информацией
57. Направления обеспечения безопасности
58. Правовые документы по защите информации и их характеристика
59. Задачи службы безопасности предприятия по обеспечению организационных мероприятий по защите информации.
60. Классификация мер инженерно-технической защиты информации.
61. Классификация программных средств защиты информации
62. Деятельность руководства предприятия и сотрудников службы безопасности по предупреждению разглашения охраняемых сведений
63. Способы пресечения разглашения информации.
64. Каналы утечки конфиденциальной информации. Их классификация. Причины и условия их возникновения.
65. Защита информации от утечки по визуально-оптическим каналам
66. Защита информации от утечки по акустическим каналам
67. Защита информации от утечки по электромагнитным каналам
68. Способы несанкционированного доступа
69. Технические средства несанкционированного доступа к информации
70. Защита от наблюдения и фотографирования
71. Способы прослушивания посредством радиозакладок. Классификация специальных радиоприемников.
72. Обеспечение безопасности телефонных переговоров

73. Назначение и характеристики нелинейных локаторов
74. Противодействие незаконному подключению к линиям связи
75. Меры защиты от радиоперехвата
76. Принципы политики информационной безопасности
77. Основные встроенные механизмы защиты ОС и их недостатки
78. Анализ существующих угроз для современных универсальных ОС
79. Оценка надежности систем защиты информации
80. Понятие добавочной защиты, способы комплексирования механизмов защиты
81. Вопросы оценки эффективности и проектирования систем защиты.
82. Сертификация ИС и ее компонентов по требованиям информационной безопасности.

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

Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме защиты курсовой работы и экзамена.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися в рамках текущего контроля баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0 до 40 от максимального количества баллов;
- «удовлетворительно» - от 41 до 60 максимального количества баллов;
- «хорошо» - от 61 до 80 максимального количества баллов;
- «отлично» - от 81 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 2.

Таблица 2 - Распределение баллов по модулям дисциплины «Комплексное обеспечение защиты информации объекта информатизации»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	10	40
Модуль – КР	100	40	60
Модуль - Экзамен	100		

Теоретический блок дисциплины оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения заданий на практических занятиях.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме защиты курсовой работы и экзамена.

Защита курсовой работы проводится по расписанию промежуточной аттестации. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Экзамен проводится по расписанию промежуточной аттестации в устном виде по экзаменационным билетам. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец экзаменационного билета

	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 И.о.зав. кафедрой ИБ» _____ А.Г.Жуковский. «___» _____ 20___ г.
Направление подготовки: 10.03.01 Информационная безопасность		
Курсы: 4		
Дисциплина: Комплексное обеспечение защиты информации объекта информатизации		
Билет №40		
1. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ. 2. Сертификация ИС и ее компонентов по требованиям информационной безопасности.		
«___» _____ 20___ г. И.о. зав. кафедрой ИБ, д.пол.н., к.т.н. доцент _____ Жуковский А.Г.		

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания по дисциплине «Комплексное обеспечение защиты информации объекта информатизации»

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций ПК-1; ПК-2.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ПК-1

Администрирование подсистем защиты информации в операционных системах

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Организационная структура службы информационной безопасности определяется: 1. Требованиями законодательства 2. Требованиями государственных и международных стандартов 3. Потребностями в защите информационных ресурсах и возможностями в соответствии с оценками руководителей предприятия
2	Аудит информационной безопасности - это: 1. Экспертное обследование различных аспектов защищенности информационных ресурсов 2. Проверка правильности оформления и учета расходов на средства защиты информации 3. Проверка уровня защищенности информационных ресурсов
3	Передача функций по обеспечению информационной безопасности на аутсорсинг обуславливается: 1. Требованиями законодательства 2. Экономической целесообразностью 3. Имиджевыми соображениями
4	Аудит информационной безопасности подразделяется на: 1. Текущий и итоговый 2. Внешний и внутренний 3. Объективный и субъективный
5	Страхование информационных рисков: 1. Обеспечивает защиту целостности и конфиденциальности информационных ресурсов 2. Позволяет компенсировать потери в случае нанесения ущерба информационным ресурсам 3. Является инструментом управления рисками
6	Риски в сфере информационной безопасности включают в себя: 1. Нарушение конфиденциальности 2. Необратимую утрату информации 3. Недоступность информационных ресурсов

№ задания	Тексты заданий
7	Лицензированием деятельности по разработке средств защиты информации в РФ занимается: 1. ФСО 2. СВР 3. ФСТЭК 4. МВД
8	Цели аудита информационной безопасности могут включать в себя: 1. Выявление лиц, нарушающих требования информационной безопасности 2. Сертификацию на соответствие общепризнанным требованиям и стандартам 3. Установление степени защищенности информационных ресурсов
9	Основой внутриобъектового режима является: 1. Режим сигнализации 2. Режим видеонаблюдения 3. Пропускной режим
10	Комплексность решения задач информационной безопасности предполагает: 1. Исключение "узких мест" в системе защиты информации 2. Анализ всех возможных сценариев нарушения безопасности и способов защиты 3. Обеспечение круглосуточной ежедневной работы службы информационной безопасности

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Сертификат безопасности свидетельствует о качествах защищенной информационной техники. Они таковы: 1. Достоверность эффективности защиты. 2. Надежность. 3. Корректность применения. Достигаются следующими действиями: А. Точным описанием порядка и области применения продукта. Б. Тестированием всех аспектов безопасности при разработке, производстве, поставке и применении продукта. В. Точным описанием защитных функций продукта в связи с характерными угрозами и наличием оценки степени устойчивости механизмов защиты.
12	Для информационной техники характерны следующие риски 1. Потеря конфиденциальности; 2. Потеря целостности; 3. Потеря функциональности, Это приводит к А. Манипуляции с данными; Б. Несанкционированное получение информации; В. Потеря или разрушение данных.
13	При определении уровня качества защиты учитываются многие факторы: 1. Корректность разработки продукта к которой относятся ...; 2. Эффективность конструкции продукта которой относятся ...; 3. Безопасность среды разработки которой относятся ...; 4. Рабочая документация которой относятся ...; 5. Область использования которой относятся А. Пригодность, совместное проявление функций, оценка уязвимых мест, стойкость механизмов защиты; Б. Требования к защищенности, архитектурный проект, подробный проект, реализация; В. Контроль конфигурации, язык программирования, компилятор, безопасность при разработке; Г. Документация пользователя, администратора системы; Д. Поставка и конфигурирование, начало использования, техническое обслуживание.
14	Для повышения надежности системы защиты информации используются три режима резервирования системы защиты дополнительными механизмами защиты: 1. Горячий резерв; 2. Активный холодный резерв; 3. Пассивный холодный резерв; Поставьте в соответствие определения данных режимов

№ задания	Тексты заданий
	А. Только одно из средств защиты (основное или дополнительное) настроено и включено. Б. Основной и дополнительный механизмы защиты настроены, но включен только один из них. В. Основные и дополнительные механизмы защиты настроены и включены.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Условно качество защищенности можно охарактеризовать по четырем уровням: низкое, удовлетворительное, хорошее, отличное. Расставьте описание уровней в порядке их повышения 1. Максимальные требования к подтверждению корректности, практически не преодолимая защита от манипуляций 2. Грубо протестированная корректность, слабая защита от манипуляций или отсутствие таковой; 3. Обстоятельно протестированная корректность, удовлетворительное действие защиты против манипуляций; 4. Тщательно протестированная корректность, хорошая или очень хорошая защита от манипуляций;
16	Расставьте в порядке повышения надежности: 1. Последовательно соединенные системы, 2. Параллельно соединенные системы или 3. Системы, имеющие смешанный вид соединения
17	Расставьте в порядке повышения эффективности поисковые устройства для обнаружения закладных электронных устройств – 1. Нелинейные локаторы, 2. Индикаторы поля, 3. Досмотровые зеркала, 4. Анализаторы спектра.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Комплекс организационно-технических мероприятий, в результате которых посредством специального документа — сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует требованиям стандартов по безопасности информации или иных нормативно-технических документов называется _____
19	К _____ средствам ИС относятся: - средства вычислительной техники общего назначения, - защищенные средства вычислительной техники, - средства связи и периферийные устройства, - локальные вычислительные сети, - глобальные вычислительные сети.
20	_____ системы защиты информации это свойство системы защиты обеспечивать защиту компьютерной информации от НСД в течение заданного промежутка времени.

Система оценивания выполнения тестовых заданий по компетенции ПК-1

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

ПК-2

Администрирование программно-аппаратных средств защиты информации в компьютерных сетях

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Информационная безопасность - это: 1. Множество факторов, влияющих на состояние информационных ресурсов 2. Уровень защищенности информационных ресурсов 3. Совокупность методов управления информационными рисками
2	Государственные органы разрабатывают и совершенствуют законодательное регулирование в сфере информационной безопасности с целью: 1. Поддержки отечественных производителей средств защиты информации 2. Обеспечения защиты государственных информационных ресурсов 3. Увеличения объема информации, циркулирующей в информационных сетях 4. Защиты интересов правообладателей
3	На формирование политики безопасности предприятия непосредственно влияют такие факторы как: 1. Требования законодательства 2. Информационная политика предприятий-конкурентов 3. Использование в работе предприятия сведений составляющих государственную или банковскую тайну
4	К задачам обучения и информационной работы с персоналом предприятия относится: 1. Недопущение утечек информации с использованием уязвимостей в сетях и ПО 2. Ознакомление с требованиями законодательства и локальных регламентов 3. Противодействие методам "социальной инженерии"
5	Долгосрочное развитие политики информационной безопасности предприятия предполагает: 1. Статичность 2. Пропорциональность 3. Цикличность
6	Основным противодействием методам "социальной инженерии" является: 1. Повышение надежности криптографических алгоритмов 2. Информационная работа с персоналом предприятия 3. Страхование информационных ресурсов
7	Меры физической защиты объектов включают в себя: 1. Укрепление помещений и бронирование дверей 2. Установку средств биометрической идентификации посетителей 3. Расположение защищаемых помещений на максимальном удалении от зон затопления 4. Ведение журнала посетителей
8	Для поддержки разработки политик безопасности используются: 1. Автоматизированные сканеры уязвимостей 2. Электронные справочные системы 3. Средства управления паролями
9	На персонал, отвечающий за обнаружение вторжений, оказывает влияние такой негативный психологический фактор как: 1. Круглосуточный режим дежурства 2. Необходимость постоянно изучать новые методы анализа вирусов 3. Частые ложные сообщения пользователей о предполагаемом заражении вирусами
10	Методы государственного управления в сфере информационной безопасности включают в себя: 1. Создание и совершенствование законодательной базы 2. Бесплатное распространение программных и аппаратных средств защиты информации 3. Осуществление международного сотрудничества в вопросах информационной безопасности

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	При разработке политики безопасности целесообразно руководствоваться следующими принципами: 1. Невозможность миновать защитные средства, 2. Недопустимость перехода в открытое состояние, 3. Минимизация привилегий; 4. Разделение обязанностей; 5. Разнообразие защитных средств. Установите соответствие принципов их описанию Д. Все информационные потоки в защищаемую сеть и из нее должны проходить через СЗИ. Г. При любых обстоятельствах СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ. В. Предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Б. Распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс А. Рекомендует организовывать различные по своему характеру оборонительные рубежи.
12	С практической точки зрения политику безопасности можно условно разделить на три уровня: верхний, средний и нижний. Установите соответствие уровней их описанию. А. вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Б. решения, затрагивающие организацию в целом. В. уровня касается конкретных сервисов.
13	Сведения, которые могут относиться к коммерческой тайне имеют категории: 1. Планы, 2. Финансы, 3. Рынок, 4. Партнеры, 5. Переговоры. Установите соответствие категорий их содержанию. А. Развитие фирмы; Б. Сведения о размерах запланированного кредитования; В. Информация о фактах подготовки и ведения переговоров; Г. Поставщики и потребители; Д. Оригинальные методы изучения рынка сбыта, состояние рынков сбыта, обзоры рынка
14	Некоторые электронные приборы, такие, как 1. Микрофоны, 2. Громкоговорители, 3. Кварцевые резонаторы, 4. Радиолампы могут служить источниками ПЭМИН. Поставьте в соответствие перечисленные приборы и принцип их действия. А. За счет механического резонанса с электрическим сигналом формирует высокостабильные радиочастотные колебания Б. Преобразует электрические колебания звуковой частоты в звук. В. Преобразует звуковые колебания в электрические. Г. Может формировать электрические колебания как генератор, усиливать их в широком диапазоне частот или работать, как переключатель.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности
Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Политика информационной безопасности описывать следующие этапы создания системы защиты информации: 1. Осуществление выбора средств защиты информации и их характеристик 2. Определение требований к системе защиты 3. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки 4. Выявление полного множества потенциально возможных угроз и каналов утечки информации 5. Определение информационных и технических ресурсов, подлежащих защите.

№ задания	Тексты заданий
16	Следующие группы людей отвечают за реализацию политики информационной безопасности: 1. Зам руководителя организации по ИБ, 2. Системные администраторы, 3. Пользователи, 4. Руководители подразделений Расставьте их в порядке иерархии в политике ИБ. 1, 2, 4, 3
17	Расставьте в порядке увеличения сложности выполняемых функций следующие сетевые устройства: 1. Шлюз, 2. Репитер, 3. Концентратор, 4. Коммутатор, 5. Маршрутизатор. 2, 3, 4, 5, 1

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	_____ (доктрина) информационной безопасности описывает основные направления, в которых государство намерено повышать уровень информационной безопасности, декларирует признание государством важность вопросов и проблем, связанных с информационной безопасностью.
19	_____, ответственного за обработку информации, включает в себя изучение приемов и методов защиты информации, необходимых для выполнения должностных обязанностей, ознакомление с возможными мерами ответственности в случае нарушения требований информационной безопасности
20	_____ — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ.

Система оценивания выполнения тестовых заданий по компетенции ПК-2

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях практического цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая практическая работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

2.3. Методические указания для обучающихся по подготовке курсовой работы

Курсовая работа включает в себя:

- титульный лист;
- содержание;
- перечень условных обозначений (при необходимости);
- основную текстовую часть работы (введение, основную часть, заключение);
- список использованных источников;
- приложения (при необходимости).

По объему страниц «Введение» может достигать 3 страниц. Во введении отражаются следующие основные моменты:

- актуальность выбранной темы,
- теоретическое и практическое значение выбранной темы, ее актуальность;
- степень разработанности проблемы (краткий обзор и анализ экономической литературы по выбранной теме курсовой работы);
- обосновывается и определяются цель, а также конкретные задачи исследования;
- обоснование логической последовательности раскрываемых вопросов, общего порядка исследования и структуры работы.

Порядок выполнения курсовой работы приведен в методических материалах по ее выполнению.

Критерии оценки курсовой работы приведены в оценочных материалах дисциплины.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся 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.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

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.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующем данному.

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 обучающихся 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 базу 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.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся 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: 84	Неделя
Модуль 1 – 42 часа			
1	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ.	5	1
2	Федеральный закон "О связи" от 07.07.2003 №126-ФЗ.	5	2
3	Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ	5	3
4	Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ.	5	4
5	Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ.	5	5
6	Закон РФ "О государственной тайне" от 21.07.1993 №5485-1.	5	6
7	Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ.	6	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	6	8
Модуль 2 – 42 часа			
9	Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11.03.1992 №2487-1	5	9
10	Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ.	5	10
11	Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ .	5	11
12	Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ.	5	12
13	Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ.	5	13
14	Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ.	5	14
15	"Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ.	6	15
16	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности	6	16

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

Самостоятельная работа обучающихся над усвоением материала по дисциплине может

выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС