

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

«28» 04 2026 г.

Рабочая программа дисциплины

**Б1.О.33 Программно-аппаратные средства защиты
информации**

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

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

Вид учебной работы	ОФО	
	ЗЕ	часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/6
Контактная работа, в том числе (по семестрам, курсам):		64/6
Лекции		32/6
Лабораторных работ		16/6
Практических занятий		16/6
Семинаров		
Самостоятельная работа		44/6
Контроль		36/6
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		
Число экзаменов с разбивкой по семестрам		1/6

Программу составил:

Кандидат технических наук, доцент Решетникова И.В.

Рабочая программа дисциплины

«Программно-аппаратные средства защиты информации»

Разработана в соответствии с ФГОС ВО

направление подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ,

утвержденное приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

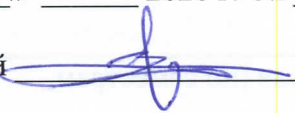
Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность», профиль «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 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины «Программно-аппаратные средства защиты информации» является формирование у обучаемых знаний в области методов и средств инженерной защиты информации, а также возможностями их использования в реальных задачах создания и внедрения инфокоммуникационных систем.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	
Знать:	- Принципы функционирования основных подсистем защиты информации в ОС (аутентификация, авторизация, контроль доступа, аудит, шифрование). - Особенности архитектуры безопасности различных операционных систем (например, модели безопасности Windows NT, концепции безопасности Linux/Unix). - Основные виды угроз безопасности операционных систем (вредоносное ПО, несанкционированный доступ, атаки на отказ в обслуживании, переполнение буфера) и типичные уязвимости. - Принципы и методы "hardening" (укрепления) операционных систем, патч-менеджмента, резервного копирования и восстановления. - Требования нормативно-правовых актов РФ и международных стандартов (например, ФЗ-152, ГОСТы, ISO 2700x) в части администрирования подсистем ЗИ в ОС. - Обзор основных инструментов и технологий для администрирования безопасности ОС (встроенные утилиты, SIEM-системы, антивирусные решения, средства управления доступом). - Взаимосвязь безопасности ОС с безопасностью сети (брандмауэры на уровне ОС).
Уметь:	- Настраивать и управлять учетными записями пользователей и группами, применять политики паролей, устанавливать права доступа (ACL) к файлам, каталогам, реестру и другим системным ресурсам. - Применять локальные и групповые политики безопасности (GPO в Windows, SELinux/AppArmor в Linux) для обеспечения требуемого уровня защищенности ОС. - Настраивать подсистемы аудита событий безопасности ОС, анализировать журналы безопасности (Event Log, Syslog) для выявления инцидентов и аномалий. - Устанавливать, настраивать и обновлять антивирусные и антишпионские средства, средства контроля целостности на уровне ОС. - Обеспечивать своевременное применение критических обновлений безопасности и патчей для операционной системы и её компонентов. - Настраивать и управлять средствами шифрования данных на дисках (например, BitLocker, LUKS) и в файловых системах (например, EFS). - Эффективно использовать командную строку (PowerShell, Bash) и графические интерфейсы для выполнения задач администрирования безопасности ОС. - Выявлять и устранять базовые проблемы и уязвимости в конфигурации безопасности операционных систем
Владеть:	- комплексными методологиями построения, администрирования и непрерывного обеспечения безопасности операционных систем на всех этапах их жизненного цикла; - проактивным мониторингом состояния безопасности ОС, оперативным реагированием на

инциденты безопасности и восстановлением после них; - системным подходом к обеспечению информационной безопасности, включая анализ рисков, планирование и внедрение защитных мер в условиях изменяющихся угроз; - способностью адаптировать и оптимизировать конфигурации безопасности ОС под специфические требования организации, отраслевые стандарты и новые угрозы; - использованием инструментов для аудита, сканирования уязвимостей и тестирования на проникновение на уровне операционной системы; - навыками администрирования систем, критически важных для безопасности информации.
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
Знать: Принципы работы и основные характеристики программно-аппаратных средств защиты информации; методы и средства обеспечения информационной безопасности в компьютерных сетях; Нормативно-правовые акты, регулирующие защиту информации; алгоритмы и протоколы шифрования данных; Основные угрозы информационной безопасности и методы их предотвращения; 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; Правила настройки и оптимизации параметров защиты в зависимости от конфигурации сети и требований к безопасности; методы тестирования на проникновение (penetration testing) и оценки уязвимостей.
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 (например, vpn); Управлять политиками безопасности в сетевых операционных системах; мониторить и анализировать журналы событий для выявления потенциальных угроз; Реагировать на инциденты безопасности и принимать меры по устранению последствий; настраивать системы обнаружения и предотвращения вторжений (ids/ips); Управлять правами доступа пользователей и групп в сети; применять политики парольной защиты и аутентификации.
Владеть: Навыками настройки и управления программными и аппаратными средствами защиты информации в компьютерных сетях; методами мониторинга и анализа событий безопасности в компьютерных сетях; Технологиями установки и настройки межсетевых экранов (файрволов), 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; Технологиями управления и контроля целостности системных файлов и настроек; методами реагирования на инциденты информационной безопасности и устранения уязвимостей.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.05 «Введение в информационные технологии»
2	Б1.О.14 «Информационные технологии и программирование»
3	Б1.О.25 «Аппаратные средства вычислительной техники»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.03 «Безопасность компьютерных сетей »
2	Б1.О.36.04 «Безопасность систем баз данных»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 64 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 6					
Модуль 1. Концепция инженерно-технической защиты информации. (16+8+8+22) часов					
1.1	Лекция 1. Основные определения и понятия. 1. Характеристика инженерно-технической защиты информации как области информационной безопасности. 2. Основные проблемы инженерно-технической защиты информации. 3. Представление сил и средств защиты информации в виде системы. 4. Основные параметры системы защиты информации	Лек	4	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2
1.2	Лекция 2. Теоретические основы инженерно-технической защиты информации. Особенности информации как предмета защиты. 1. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. 2. Принципы защиты информации техническими средствами.	Лек	4	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2
1.3	Лекция 3. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.	Лек	4	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2
1.4	Лекция 3. Характеристика технической разведки Основные задачи и органы технической разведки. Демаскирующие признаки радиоэлектронных средств Виброакустические технические каналы утечки речевой информации	Лек	4	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2
1.5	Практическая работа 1. Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации	ПЗ	4	ОПК-1.4	Л3.1

1.6	Практическая работа 2. Изучение задач и функций органов по технической защите информации в РФ	ПЗ	4	ОПК-1.4	ЛЗ.1
1.7	Лабораторная работа №1. Организация аттестации выделенного помещения по требованиям безопасности информации	ЛР	4	ОПК-1.4	ЛЗ.1
1.8	Лабораторная работа №2. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении	ЛР	4	ОПК-1.4	ЛЗ.1
1.9	Демаскирующие признаки объектов Параметрические технические каналы утечки речевой информации Акустоэлектрические каналы утечки речевой информации Демаскирующие признаки объектов в видимом диапазоне Демаскирующие признаки объектов в инфракрасном диапазоне	СРС	22	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2
Модуль 2 Технический контроль эффективности мер защиты информации (16+8+8+22) часов					
2.1	Лекция 5. Общие вопросы организации противодействия технической разведке. 1. Основные организационные и технические мероприятия, используемые для противодействия технической разведке. 2. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам. 3. Физические основы образования побочных электромагнитных излучений от технических средств.	Лек	4	ОПК-10	Л1.1 Л1.2 Л2.1 Л2.2
2.2	Лекция 6. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. 1. Основные этапы доступа к ресурсам вычислительной системы.	Лек	4	ОПК-10	Л1.1 Л1.2 Л2.1 Л2.2
2.3	Лекция 7. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам. 1. Использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания.	Лек	4	ОПК-10	Л1.1 Л1.2 Л2.1 Л2.2
2.4	Лекция 8. Цели и задачи технического контроля эффективности мер защиты информации 1. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ 2. Порядок проведения контроля защищенности АС от НСД 3. Методы контроля побочных электромагнитных излучений генераторов технических средств	Лек	4	ОПК-10	Л1.1 Л1.2 Л2.1 Л2.2
2.4	Практическое занятие №3 Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	ПЗ	4	ОПК-10	ЛЗ.1
2.5	Практическое занятие № 4 Изучение положения о сертификации средств вычислительной техники и связи	ПЗ	4	ОПК-10	ЛЗ.1
2.7	Лабораторная работа № 3 «Исследование детектора электромагнитного поля ST107».	ЛР	4	ОПК-10	ЛЗ.1

2.8	Лабораторная работа № 4 Обнаружение сигналов линейных и сетевых закладок	ЛР	4	ОПК-10	ЛЗ.1
2.9	Способы предотвращения утечки информации через ПЭМИН ПК Методы средства ограничения доступа к компонентам ЭВМ Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления	СРС	22	ОПК-10	Л1.1 Л1.2 Л2.1 Л2.2
	Экзамен		36	ОПК-10 ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2 ЛЗ.1
Итого – 144 часа					

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	Зайцев А.П., Мещеряков Р.Е., Шелупанов А.А.	Технические средства и методы защиты информации.	Учебник для вузов. 7-е изд., перераб. и доп. - 2024	Э1
Л1.2	Милославская Н.Г., Толстой А.И.	Межсетевые экраны	. Учебное пособие для вузов. - Москва : Горячая линия - Телеком,.2024	Э2
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Киселев Д.Н., Перфилов О.Ю.	Радиомониторинг и распознавание радиоизлучения.	Учебное пособие для вузов. - Москва : Горячая линия - Телеком,.2023	Э3
Л2.1	Нагаев Н.Х.	Антивирусная безопасность цифровой информации.	Учебное пособие для вузов. - Москва : Горячая линия - Телеком,.2024	Э4
5.1.3 Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	Решетникова И.В	Программно-аппаратные средства защиты информации сетей и систем. Учебное пособие.	РнД: СКФ МТУСИ, 2024. – 52 с.	Э5
5.2 Электронные образовательные ресурсы				
Э1	https://elib.mtuci.ru/view.php?book_id=4112			
Э2	https://elib.mtuci.ru/view.php?book_id=34676			

Э3	https://elibr.mtuci.ru/view.php?book_id=3865
Э4	https://elibr.mtuci.ru/view.php?book_id=34655
Э5	https://elibr.mtuci.ru/view.php?book_id=170086
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	Сборник нормативных документов «Регламент» – https://reglament.pro/index.php/entrance (неограниченный доступ для авторизованных пользователей)
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)
5.4 Программное обеспечение	
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:	
П.1	DFLAS LOCK
П.2	Сканер BE
П.3	КИБ Серчинформ
П.4	Kali Linux
П.5	VIP NET
П.	MS Office 2016

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная 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
2	Лаборатория «Технической защиты информации», укомплектованная специализированной мебелью, оснащенная техническими средствами защиты информации
3	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.3 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, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.О.33 Программно-аппаратные средства защиты информации» 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
ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями		
Знать:		
• Принципы функционирования основных подсистем защиты информации в ОС (аутентификация, авторизация, контроль доступа, аудит, шифрование). • Особенности архитектуры безопасности различных операционных систем (например, модели безопасности Windows NT, концепции безопасности Linux/Unix). • Основные виды угроз безопасности операционных систем (вредоносное ПО, несанкционированный доступ, атаки на отказ в обслуживании, переполнение буфера) и типичные уязвимости. • Принципы и методы "hardening" (укрепления) операционных систем, патч-менеджмента, резервного копирования и восстановления. • Требования нормативно-правовых актов РФ и международных стандартов (например, ФЗ-152, ГОСТы, ISO 2700x) в части администрирования подсистем ЗИ в ОС. • Обзор основных инструментов и технологий для администрирования безопасности ОС (встроенные утилиты, SIEM-системы, антивирусные решения, средства управления доступом). • Взаимосвязь безопасности ОС с безопасностью сети (брандмауэры на уровне ОС).	Контрольная работа 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» -9-10
Уметь		
• Настраивать и управлять учетными записями пользователей и группами, применять политики паролей, устанавливать права доступа (ACL) к файлам, каталогам, реестру и другим системным ресурсам. • Применять локальные и групповые политики безопасности (GPO в Windows, SELinux/AppArmor в Linux) для обеспечения требуемого уровня защищенности ОС. • Настраивать подсистемы аудита событий безопасности ОС,	Лабораторные работы 1-2	Модуль 1 0÷8 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-4 «Хорошо» - 5-6 «Отлично» - 7-8

анализировать журналы безопасности (Event Log, Syslog) для выявления инцидентов и аномалий. • Устанавливать, настраивать и обновлять антивирусные и антишпионские средства, средства контроля целостности на уровне ОС. • Обеспечивать своевременное применение критических обновлений безопасности и патчей для операционной системы и её компонентов. • Настраивать и управлять средствами шифрования данных на дисках (например, BitLocker, LUKS) и в файловых системах (например, EFS). • Эффективно использовать командную строку (PowerShell, Bash) и графические интерфейсы для выполнения задач администрирования безопасности ОС. • Выявлять и устранять базовые проблемы и уязвимости в конфигурации безопасности операционных систем		
Владеть		
• Комплексными методологиями построения, администрирования и непрерывного обеспечения безопасности операционных систем на всех этапах их жизненного цикла. • Проактивным мониторингом состояния безопасности ОС, оперативным реагированием на инциденты безопасности и восстановлением после них. • Системным подходом к обеспечению информационной безопасности, включая анализ рисков, планирование и внедрение защитных мер в условиях изменяющихся угроз. • Способностью адаптировать и оптимизировать конфигурации безопасности ОС под специфические требования организации, отраслевые стандарты и новые угрозы. • Использованием продвинутых инструментов для аудита, сканирования уязвимостей и тестирования на проникновение на уровне операционной системы. • навыками администрирования систем, критически важных для безопасности информации	Практические занятия 1-3	Модуль 1 0÷8 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-4 «Хорошо» - 5-6 «Отлично» - 7-8

ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты, системы подвижной связи различного назначения		
Знать:		
Принципы работы и основные характеристики программно-аппаратных средств защиты информации; методы и средства обеспечения информационной безопасности в компьютерных сетях; Нормативно-правовые акты, регулирующие защиту информации; алгоритмы и протоколы шифрования данных; Основные угрозы информационной безопасности и методы их предотвращения; 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; Правила настройки и оптимизации параметров защиты в зависимости от конфигурации сети и требований к безопасности; методы тестирования на проникновение (penetration testing) и оценки уязвимостей;	Контрольная работа	Модуль 2 0÷10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
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 (например, vpn); Управлять политиками безопасности в сетевых операционных системах; мониторить и анализировать журналы событий для выявления потенциальных	Лабораторные работы 3-4	Модуль 2 0÷8 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-4 «Хорошо» - 5-6 «Отлично» - 7-8

угроз; Реагировать на инциденты безопасности и принимать меры по устранению последствий; настраивать системы обнаружения и предотвращения вторжений (ids/ips); Управлять правами доступа пользователей и групп в сети; применять политики парольной защиты и аутентификации;		
Владеть		
Навыками настройки и управления программными и аппаратными средствами защиты информации в компьютерных сетях; методами мониторинга и анализа событий безопасности в компьютерных сетях; Технологиями установки и настройки межсетевых экранов (файрволлов), 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; Технологиями управления и контроля целостности системных файлов и настроек; методами реагирования на инциденты информационной безопасности и устранения уязвимостей.	Практические занятия 4-6	Модуль 2 0÷8 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-4 «Хорошо» - 5-6 «Отлично» - 7-8
	Экзамен	0-100 «Неудовлетворительно» 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы 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 3 лекционных занятия и 2 ЛР и 3 ПЗ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные ЛР или ПЗ обучающийся получает максимум 8 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ОПК-1.4):

1. Характеристика инженерно-технической защиты информации как области информационно-безопасности.
2. Основные проблемы инженерно-технической защиты информации.
3. Представление сил и средств защиты информации в виде системы.
4. Основные параметры системы защиты информации
5. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.
6. Принципы защиты информации техническими средствами.
7. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.
8. Кто является основным ответственным за определение уровня классификации информации?
9. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
10. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
11. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
12. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
13. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
14. Что такое политики безопасности?

Практическое занятие №1 Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации (ОПК-1.4)

Контрольные вопросы:

Назовите основные виды конфиденциальной информации.

Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?

Охарактеризуйте место правовых мер в системе комплексной защиты информации.

Назовите интересы государства в области обеспечения информационной безопасности.

Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.

Какой закон определяет понятие «официальный документ»?

Какой закон определяет понятие «электронный документ»?

В каком законе приведена классификация средств защиты информации?

Назовите основные положения Доктрины информационной безопасности РФ.

Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?

Дайте определение системы защиты государственной тайны и укажите ее составляющие.

Что в соответствии с законодательством РФ представляет собой засекречивание информации.

Перечислите основные принципы засекречивания информации.

Что понимается под профессиональной тайной?

Какие виды профессиональных тайн вам известны?

Что представляет собой электронная подпись?

Практическое занятие №2

Изучение задач и функций органов по технической защите информации в РФ (ОПК-1.4)

Контрольные вопросы:

1. Перечислите органы государственного регулирования и контроля в области информационной безопасности РФ. Каковы основные направления их деятельности?

2. Какие организации в области технической защиты информации являются ключевыми органами?

3. Назовите документы, которым руководствуется ФСБ России в своей деятельности?

3. Перечислите основные задачи ФСБ в области технической защиты информации.

4. Перечислите основные функции ФСБ в области технической защиты информации.

5. В каком случае ФСБ России имеет право проводить плановые проверки?

6. Перечислите основные задачи ФСТЭК в области технической защиты информации.

7. Перечислите основные функции ФСТЭК в области технической защиты информации.

8. Каковы полномочия ФСТЭК?

Практическое занятие №3 Изучение положений о государственном лицензировании деятельности в области защиты информации (ОПК-1.4)

Контрольные вопросы:

Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.

Организационная структура системы государственного лицензирования в области защиты информации.

Функции государственных органов по лицензированию в области защиты информации.

Функции лицензионных центров по лицензированию в области защиты информации.

Права и обязанности лицензиатов.

Порядок проведения лицензирования и контроля за деятельностью лицензиатов.

Назовите случаи приостановления или прекращения действия лицензии.

В каких случаях предприятию отказывают в выдаче лицензии?

Какие документы предоставляются для получения лицензии?

Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

Какие средства относятся к шифровальным?

Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Лабораторная работа №1. Организация аттестации выделенного помещения по требованиям безопасности информации. (ОПК-1.4)

Порядок выполнения работы

Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Изобразить план-схему исследуемого помещения.

На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металлодетектора.

Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Контрольные вопросы

1. Средства акустического контроля.
2. Аппаратура для съема информации с окон.
3. Специальная звукозаписывающая аппаратура.
4. Микрофоны различного назначения и исполнения.
5. Электросетевые подслушивающие устройства.
6. Приборы для съема информации с телефонной линии связи и сотовых телефонов.
7. Специальные системы наблюдения и передачи видеоизображений.
8. Специальные фотоаппараты.
9. Приборы наблюдения в дневное время и приборы ночного видения.
10. Специальные средства радиоперехвата и приема ПЭМИН и др

Лабораторная работа №2. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении. (ОПК-1.4)

Порядок выполнения работы

Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Изобразить план-схему исследуемого помещения.

На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металлодетектора.

Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Контрольные вопросы

1. Приведите определение закладочного устройства.
2. Перечислите демаскирующие признаки автономных некамуфлированных акустических закладок.
3. Перечислите демаскирующие признаки полуактивных акустических радиозакладок.
4. Какие технические средства применяют для выявления радиозакладочных устройств?
5. Назначение комплекса «RS turbo Mobile-L».
6. Перечислите состав комплекса «RS turbo Mobile-L».
7. Радиозакладки с каким видом модуляции обнаруживает комплекс RS turbo?

Модуль 2: (50 баллов):

Модуль содержит 3 лекционных занятия и 2 ЛР и 3 ПЗ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные ЛР или ПЗ обучающийся получает максимум 8 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 2 (ОПК-10):

1. Основные организационные и технические мероприятия, используемые для противодействия технической разведке.
2. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам;
3. Физические основы образования побочных электромагнитных излучений от технических средств.
4. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.
5. Базовые этапы построения системы комплексной защиты вычислительных систем.
6. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.
7. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
8. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля.
9. Взаимная проверка подлинности и другие случаи опознавания.
10. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.

11. Виды информации с точки зрения информационной безопасности.
12. Виды защищаемой информации.
13. Интересы личности (общества, государства) в информационной сфере.
14. Проблемы региональной информационной безопасности.
15. Основные нормативно-правовые акты в области информационной безопасности.
16. Исторические этапы развития системы защиты информации в России.

Лабораторная работа № 3

Исследование детектора электромагнитного поля ST107 (ОПК-10)

Порядок выполнения работы

По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации детектора электромагнитного поля ST107 и меры безопасности при работе с ним.

Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов.

Провести обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями детектора электромагнитного поля ST107.

Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию с использованием и без использования частотомера.

Составить отчет о проделанной работе, который должен включать:

описание индикатора, принципа его действия, характеристик и основных приемы работы;

данные, полученные при исследовании ЭМО в лаборатории;

результаты идентификации контрольных образцов с подробным обоснованием принятого решения.

Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме.

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Лабораторная работа № 4

Обнаружение сигналов линейных и сетевых закладок (ОПК-10)

Порядок выполнения работы

Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Изобразить план-схему исследуемого помещения.

На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металлодетектора.

Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Контрольные вопросы (ОПК-10):

1. Специальные исследования акустических и виброакустических каналов.
2. Специальные исследования акустоэлектрических преобразований
3. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок
4. Объекты защиты информации
5. Охраняемые сведения и демаскирующие признаки
6. Технические каналы утечки информации
7. Причины образования технических каналов утечки информации
8. Прямой перехват сигналов

Практическое занятие №4. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации (ОПК-10)

Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Какова организационная структура системы сертификации средств защиты информации по требованиям безопасности информации?
3. Назовите виды и схемы сертификации средств защиты информации.
4. Каковы функции ФСТЭК в области сертификации средств защиты информации?
5. Каковы функции органов сертификации средств защиты информации?
6. Каковы функции испытательных лабораторий (центров)?
7. Каковы функции заявителей?
8. Каков общий порядок проведения сертификации средств защиты информации.
9. Перечислите виды контроля в области сертификации средств защиты информации?
10. Чем определяются сроки проведения сертификационных испытаний?
11. На какой срок выдается сертификат?
12. Назовите причины приостановления или аннулирования действия сертификата.

Практическое занятие № 5

Изучение положения о сертификации средств вычислительной техники и связи (ОПК-10)

Контрольные вопросы

1. Какова организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации?
2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Каковы особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Перечислите виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.

6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.

Практическое занятие № 6

Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации (ОПК-10)

Контрольные вопросы

1. Назовите цели и задачи испытаний и проверок.
2. Каковы условия проведения испытаний?
3. Перечислите общие методы испытаний.
4. В чем состоит суть испытаний объектов на соответствие организационно-техническим требованиям по защите информации?
5. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН?
6. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания?
7. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи?
8. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от НСД?
9. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по акустическим каналам?
10. В чем состоит суть проверки выполнения требований по защите информации от утечки за счет встроенных технических средств?
11. В чем состоит суть проверки правильности применения криптографических средств защиты информации?
12. Каким образом осуществляется оценка результатов испытаний и оформление отчетных материалов?

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Программно-аппаратные средства защиты информации» (ОПК-1.4, ОПК-10) (промежуточная аттестация):

1. Виды, источники и носители защищаемой информации
2. Классификация иностранной технической разведки. Возможности видов технической разведки
3. Основные этапы и процедуры добывания информации технической разведкой
4. Задачи систем защиты информации
5. Технические каналы утечки информации. Структура, классификация и основные характеристики
6. Контроль и прослушивание телефонных каналов связи
7. Технические каналы утечки речевой информации
8. Акустические каналы утечки речевой информации Направленные микрофоны Виды направленных микрофонов .
9. Виброакустические технические каналы утечки речевой информации .
10. Оптико-электронный технический канал утечки речевой информации .
11. Технические каналы утечки видовой информации. Способы скрытого видеонаблюдения и съемки .
12. Технические каналы утечки видовой информации .

13. Способы скрытого видеонаблюдения и съемки .
14. Демаскирующие признаки объектов .
15. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра .
16. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра .
17. Демаскирующие признаки радиоэлектронных средств .
18. Индикаторы электромагнитного поля .
19. Сканирующие радиоприемники .
20. Анализаторы спектра, радиочастотомеры .
21. Многофункциональные комплекты для выявления каналов утечки информации .
22. Нелинейные локаторы .
23. Металлодетекторы .
24. Портативная рентгенотелевизионная установка .
25. Досмотровые эндоскопы .
26. Скрытие речевой информации в телефонных системах с использованием криптографических методов .
27. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах .
28. Методы и средства инженерной защиты и технической охраны объектов .
29. Категории объектов защиты .
30. Особенности задач охраны различных типов объектов .
31. Общие принципы обеспечения безопасности объектов .
32. Система охранно-тревожной сигнализации .
33. Система контроля и управления доступом .
34. Телевизионные системы .
35. Система пожарной сигнализации .
36. Периметровая охрана .
37. Аттестация объектов информатизации .
38. Мероприятия по выявлению и оценке свойств каналов утечки информации .
39. Специальные проверки .
40. Специальные обследования .
41. Специальные исследования .
42. Специальные исследования акустических и виброакустических каналов .
43. Специальные исследования акустоэлектрических преобразований .
44. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок .
45. Объекты защиты информации .
46. Охраняемые сведения и демаскирующие признаки .
47. Технические каналы утечки информации .
48. Причины образования технических каналов утечки информации .
49. Прямой перехват сигналов .
50. Нежелательные излучения радиопередающих устройств систем связи и передачи информации .
51. Нежелательные излучения технических средств обработки информации .
52. Нежелательные электромагнитные связи .
53. Излучатели электромагнитных полей .
54. Утечка информации по цепям заземления .
55. Утечка информации по цепям питания .
56. Высокочастотное навязывание .
57. Утечка информации по акустическим каналам .
58. Прямой акустический канал .
59. Виброакустический канал .

60. Оптико-акустический канал .
61. Электроакустический канал .
62. Утечка информации в волоконно-оптических линиях связи .
63. Экранирование электромагнитных полей .
64. Экранирование электрических полей .
65. Экранирование магнитных полей .
66. Экранирование проводов и соединительных линий .
67. Материалы для экранов .
68. Фильтрация .
69. Заземление технических средств .

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 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 обучающимися 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 баллы в рамках текущего контроля 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 обучающимися по блокам

модулей, показаны в Таблице.

Таблица 1 - Распределение баллов по блокам модулей дисциплины «Программно-аппаратные средства защиты информации»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	10	40
Модуль 2	50	10	40
Экзамен	100		100

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

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

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена. 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: 3 Дисциплина: <i>Программно-аппаратные средства защиты информации</i>	
Билет №1 1. Причины образования технических каналов утечки информации 2. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах к.т.н., доцент _____ Решетникова И.В. «___» _____ 20__ 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, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций **ОПК-1.4, ОПК-10**.

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.

ОПК-1.4: 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	В каких единицах измеряется риск? 1. в стоимостном выражении 2. во временном выражении 3. процентах 4. в уровнях
2	Анализ информационных рисков предназначен для: 1. оценки существующего уровня защищенности информационной системы и формирования оптимального бюджета на информационную безопасность; 2. оценки технического уровня защищенности информационной системы 3. получения стоимостной оценки вероятного финансового ущерба от реализации угроз, направленных на информационную систему компании и для оценки возможности реализации угроз 4. убеждения руководства компании в необходимости вложений в систему обеспечения ИБ и для инструментальной проверки защищенности информационной системы
3	Политика информационной безопасности необходима для: 1. успешного прохождения компанией регулярного аудита по ИБ 2. обеспечения реального уровня защищенности ИС компании 3. понимания персоналом важности требований по ИБ 4. обеспечения адекватной защиты наиболее важных ресурсов компании
4	Политика информационной безопасности в общем случае является: 1. руководящим документом для администраторов безопасности и системных администраторов 2. руководящим документом для ограниченного использования

№ задания	Тексты заданий
	3. руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов 4. руководящим документом для всех сотрудников компании
5	Выберите, невыполнение, какого из следующих требований политики безопасности может наибольшим образом повысить существующие в системе информационные риски: 1. регулярное обновление антивирусных баз 2. создание и поддержание форума по информационной безопасности для всех специалистов, вовлеченных в процесс обеспечения ИБ 3. классификация ресурсов по степени важности с точки зрения ИБ 4. завершение активной сессии пользователя по окончании работы
6	Международный стандарт управления ИБ ISO 27001 предъявляет: 1. требования, предъявляемые только для узкого круга крупнейших мировых компаний 2. базовые требования по обеспечению ИБ 3. повышенные требования по обеспечению безопасности информационной системы 4. требования, которые не соответствуют законам стран СНГ в области ИБ
7	Одной из рекомендаций ISO 27001 является: 1. четкая регламентация настроек межсетевых экранов 2. применение антивирусных продуктов ведущих производителей 3. проведение анализа рисков и регулярных тестов на проникновение сторонней компанией 4. необходимость прохождения руководством компании регулярных тренингов по ИБ
8	Для проведения анализа информационных рисков необходимо: 1. градация информационных рисков 2. построение полной модели информационной системы с точки зрения ИБ 3. модель нарушителя 4. вероятностные оценки угроз безопасности
9	Основной задачей теста на проникновение является: 1. оценка возможности обнаружения атаки службой ИБ компании 2. проверка времени реакции службы обеспечения информационной безопасности 3. оценка возможности осуществления атаки из Интернет на информационную систему компании 4. оценка возможных потерь при реализации атаки из Интернет
10	Тест на проникновение позволяет: 1. убедить руководство компании в реальной опасности вторжения из Интернет и обосновать необходимость инвестиций в ИБ 2. снизить вероятные риски вирусной атаки на корпоративную сеть 3. обеспечить должный уровень отношения руководства компании к проблеме обеспечения ИБ 4. убедиться в способности службы ИБ противостоять возможным атакам злоумышленников из Интернет

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

№ задания	Тексты заданий
11	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. Анализ рисков 2. Модель угроз 3. Техническое задание (ТЗ) 4. Техно-экономическое обоснование А. Оценка стоимости внедрения и эксплуатации системы защиты информации Б. Определение уязвимостей в проектируемой системе. В. Идентификация потенциальных угроз и оценка их вероятности и воздействия Г. Документ, определяющий функциональные и нефункциональные требования к подсистеме защиты информации..
12	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику.

№ задания	Тексты заданий
	1. Архитектура сети 2. Нормативные требования 3. Популярные типы атак 4. Уровень осведомленности персонала А. Интервью с сотрудниками службы безопасности и сетевыми администраторами. Б. Анализ документации, внутренних регламентов и политик компании. В. Сканирование сети с использованием специализированных инструментов. Г. Изучение отчетов об инцидентах, новостей и аналитических статей по информационной безопасности
13	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. Межсетевой экран 2. Антивирусное ПО 3. Система обнаружения вторжений (IDS) 4. Средства резервного копирования А. Обеспечение целостности данных. Б. Выявление и блокировка вредоносного программного обеспечения. В. Контроль и фильтрация сетевого трафика. Г. Обнаружение аномальной активности в сети.
14	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. Вероятность реализации угрозы 2. Ущерб от реализации угрозы 3. Производительность системы защиты 4. Стоимость владения системой А. Рубли (или другая валюта). Б. Проценты (%). В. Событий в секунду (EPS), пакетов в секунду (PPS) Г. Безразмерная величина (от 0 до 1 или вероятность в долях единицы).

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

Инструкция: Расположите предложенные элементы в правильной последовательности, соответствующей логическому порядку выполнения действий или этапов процесса.

№ задания	Тексты заданий
15	Этапы разработки технического задания (ТЗ) на подсистему защиты информации Расположите этапы разработки технического задания в правильном порядке: 1. Согласование и утверждение ТЗ. 2. Разработка структуры и содержания ТЗ. 3. Сбор и анализ требований к системе защиты информации. 4. Рецензирование и корректировка проекта ТЗ
16	Процесс анализа информационных рисков Расположите этапы анализа информационных рисков в правильном порядке: 1. Оценка ущерба от реализации угроз. 2. Идентификация активов, угроз и уязвимостей. 3. Определение вероятности реализации угроз. 4. Разработка и внедрение мер по управлению рисками.

№ задания	Тексты заданий
17	Подготовка технико-экономического обоснования (ТЭО) для проекта по информационной безопасности Расположите этапы подготовки ТЭО в правильном порядке: 1. Оценка затрат на внедрение и эксплуатацию системы защиты информации. 2. Определение целей и задач проекта по информационной безопасности. 3. Сравнение затрат и выгод от реализации проекта. 4. Определение перечня необходимых средств защиты информации

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом
Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Добавить недостающие слова в определение доступа к информации: Для эффективной оценки рисков необходимо собрать и проанализировать _____ о существующих _____ и _____ в информационной системе.
19	Добавить недостающие слова в определение доступа к информации: При подготовке технико-экономического обоснования (ТЭО) важно учитывать не только прямые _____ на внедрение системы защиты, но и потенциальные _____ от предотвращения инцидентов.
20	Добавить недостающие слова в определение доступа к информации: Перед проектированием подсистемы защиты данных необходимо определить _____ пользователей и уровни _____ к информации, чтобы разработать адекватные механизмы аутентификации и авторизации.

Система оценивания выполнения тестовых заданий по компетенции ОПК-1.4

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.

ОПК-10: Способен разрабатывать, проектировать, внедрять и эксплуатировать объекты и системы связи, телекоммуникационные системы, системы подвижной связи различного назначения

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	Какой тип модуляции чаще всего используется в сетях Wi-Fi (802.11)? 1. Частотная модуляция (FM) 2. Амплитудная модуляция (AM) 3. Квадратурная амплитудная модуляция (QAM) 4. Фазовая модуляция (PM)
2	Что такое ММО в контексте телекоммуникаций? 1. Метод шифрования данных. 2. Технология множественного входа и множественного выхода. 3. Протокол маршрутизации в сети. 4. Тип оптического волокна.
3	Какой протокол используется для обеспечения безопасной передачи данных по сети Интернет? 1. HTTP 2. FTP 3. SMTP 4. HTTPS
4	Что такое VoLTE? 1. Голосовая связь только через Wi-Fi. 2. Технология передачи голоса по сети LTE. 3. Протокол для передачи видеоконтента в высоком разрешении. 4. Система управления базовыми станциями сотовой связи.
5	Какая топология сети характеризуется наличием центрального узла, к которому подключены все остальные узлы? 1. Шина 2. Кольцо 3. Звезда 4. Ячеистая
6	Что такое OFDM в контексте беспроводных технологий? 1. Метод шифрования данных. 2. Схема множественного доступа с кодовым разделением. 3. Мультиплексирование с ортогональным частотным разделением. 4. Протокол управления сетевыми устройствами.
7	Какой тип кабеля обычно используется для подключения абонентов к сети Интернет по технологии PON? 1. Коаксиальный кабель 2. Витая пара 3. Оптическое волокно 4. Силовой кабель
8	Что такое SDN (Software Defined Networking)? 1. Тип операционной системы для серверов. 2. Архитектура сети, где управление логикой сети отделено от устройств передачи данных.

№ задания	Тексты заданий
	3. Протокол для обмена сообщениями между сетевыми устройствами. 4. Метод сжатия видеоконтента.
9	Какой параметр характеризует пропускную способность канала связи? 1. Задержка 2. Джиттер 3. Полоса пропускания 4. Потери пакетов
10	Что такое роуминг в сетях мобильной связи? 1. Процесс автоматического переключения между сетями разных операторов. 2. Процедура ручной настройки параметров сети. 3. Технология оптимизации энергопотребления мобильного устройства. 4. Метод защиты от несанкционированного доступа к сети.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Для каждого элемента выберите соответствующий элемент который наиболее точно описывает его назначение или характеристику.

№ задания	Тексты заданий
11	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. SIP 2. Bluetooth 3. LTE 4. GPON А. Стандарт беспроводной связи для обмена данными на коротких расстояниях. Б. Протокол сигнализации, используемый для установления, управления и завершения сеансов в IP-телефонии. В. Технология беспроводной широкополосной связи, используемая в мобильных сетях четвертого поколения (4G). Г. Технология пассивной оптической сети, используемая для предоставления высокоскоростного доступа в Интернет.
12	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. Маршрутизатор 2. Коммутатор 3. Медиаконвертер 4. Точка доступа (Access Point) А. Устройство, которое преобразует электрические сигналы в оптические и наоборот Б. Устройство, которое пересылает пакеты данных между различными сетями, выбирая оптимальный маршрут. В. Устройство, которое соединяет несколько устройств в одной сети, пересылая данные только на нужный порт. Г. Устройство, которое обеспечивает беспроводное подключение к сети, позволяя беспроводным устройствам подключаться к проводной сети.
13	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. Полоса пропускания 2. Задержка 3. Мощность сигнала 4. Коэффициент ошибок по битам (BER) А. dBm (децибел-милливатт)

№ задания	Тексты заданий
	Б. Бит в секунду (bps) или его производные (Kbps, Mbps, Gbps) В. Миллисекунды (ms) Г. Безразмерная величина (отношение количества ошибочных битов к общему количеству переданных битов)
14	Для каждого элемента выберите соответствующий элемент из, который наиболее точно описывает его назначение или характеристику. 1. Межсетевой экран (Firewall) 2. VLAN 3. VPN 4. SRTP 5. Система обнаружения вторжений (IDS) А. Обеспечивает конфиденциальность разговоров в сетях VoIP, шифруя голосовой трафик. Б. Система, анализирующая сетевой трафик в реальном времени для выявления атак и подозрительной активности В. Разделяет физическую сеть на логические подсети, повышая безопасность и управляемость трафика Г. Контролирует и фильтрует сетевой трафик, блокируя несанкционированный доступ к сети и защищая от внешних угроз Д. Создает защищенное соединение через общедоступную сеть, обеспечивая безопасную передачу данных между двумя точками, часто используется для удаленного доступа.

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

Инструкция: Расположите предложенные элементы в правильной последовательности, соответствующей логическому порядку выполнения действий или этапов процесса

№ задания	Тексты заданий
15	Процесс внедрения новой системы VoIP в организации с обеспечением безопасности Расположите этапы внедрения VoIP в правильном порядке, уделяя внимание безопасности: 1. Настройка межсетевого экрана для фильтрации VoIP-трафика. 2. Анализ рисков безопасности VoIP-коммуникаций (например, прослушивание, фрод). 3. Внедрение и настройка серверов VoIP. 4. Внедрение SRTP (Secure Real-time Transport Protocol) для шифрования голосового трафика.
16	Процесс анализа информационных рисков Расположите этапы анализа информационных рисков в правильном порядке: 1. Оценка ущерба от реализации угроз. 2. Идентификация активов, угроз и уязвимостей. 3. Определение вероятности реализации угроз. 4. Разработка и внедрение мер по управлению рисками.
17	Этапы проектирования защищенной беспроводной сети (Wi-Fi) Расположите этапы проектирования безопасной Wi-Fi сети в правильном порядке: 1. Выбор оборудования с поддержкой современных протоколов шифрования (WPA3). 2. Проведение анализа покрытия и планирование размещения точек доступа. 3. Настройка параметров безопасности (шифрование, аутентификация, фильтрация MAC-адресов). 4. Оценка рисков и определение требований к безопасности беспроводной сети.

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Добавить недостающие слова в определение доступа к информации: Использование _____ в сетях подвижной связи позволяет повысить эффективность использования радиочастотного спектра и увеличить пропускную способность сети для большего числа пользователей.
19	Добавить недостающие слова в определение доступа к информации: Использовать _____ для защиты от атак типа "отказ в обслуживании" (DDoS) в телекоммуникационных сетях. Опишите механизмы обнаружения и фильтрации атак, а также преимущества и недостатки различных подходов
20	Добавить недостающие слова в определение доступа к информации: Для обеспечения конфиденциальности ключей шифрования в телекоммуникационной системе необходимо использовать комплексный подход, включающий следующие методы и технологии: _____, _____,

Система оценивания выполнения тестовых заданий по компетенции ОПК-10

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 лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная 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 лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 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.

Для подготовки и выполнения лабораторных работ используется учебное пособие: ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ СЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2022. – 52 с. в разделе «Методические материалы»: http://www.skf-mtusi.ru/?page_id=659.

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.

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, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Обучающимся очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1 настоящей рабочей программы, рекомендуется соблюдать последовательность их изучения, представленную в таблице.

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 и др.	Часов всего: 44
Модуль 1		22
1	Параметрические технические каналы и акустоэлектрические каналы	2
2	Параметрические технические каналы утечки речевой информации	2
3	Акустоэлектрические каналы утечки речевой информации	2
4	Демаскирующие признаки объектов	4
5	Демаскирующие признаки объектов в видимом диапазоне	4
6	Демаскирующие признаки объектов в инфракрасном диапазоне	2
7	Параметрические технические каналы и акустоэлектрические каналы	2
8	Параметрические технические каналы утечки речевой информации	4

Модуль 2		22
1	Способы предотвращения утечки информации через ПЭМИН ПК	2
2	Методы средства ограничения доступа к компонентам ЭВМ	4
3	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	4
4	Безопасность оптоволоконных кабельных систем.	4
5	Заземление технических средств и подавление информационных сигналов в цепях заземления	4
6	Подготовка к экзамену	4

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.