

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


«31» 03

Н.А. Андреева

2025 г.

Б1.О.36.05 Методы оценки безопасности компьютерных систем
(Аудит компьютерных систем)
рабочая программа дисциплины

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

Вид учебной работы	ОФО	
	ЗЕ	часов/сем.
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/7
Контактная работа, в том числе (по семестрам, курсам):		84/7
Лекции		34/7
Лабораторных работ		34/7
Практических занятий		16/7
Семинаров		
Самостоятельная работа		60/7
Контроль		36/7
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		1/7
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		
Число экзаменов с разбивкой по семестрам (курсам)		1/7

Программу составил:

доцент кафедры ИВТ к.т.н. доцент Маршаков Д.В.

Рабочая программа дисциплины

«Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)»

Разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427

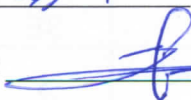
Составлена на основании учебных планов

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 2025, и утвержденного директором СКФ МТУСИ 31.03 2025 г.

Рассмотрена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от 31 марта 2025 г. № 8.

И.о.зав. кафедрой



Жуковский А.Г.

1. Цели изучения дисциплины

Целями изучения дисциплины "*Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)*" является получение обучающимися знаний о процедурах аудита информационной безопасности защищённых автоматизированных систем и организаций, методах сбора и анализа свидетельств аудита информационной безопасности и их оценке и умений по разработке и применению методик информационной безопасности автоматизированных 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:

Компетенции, формируемые у обучающегося в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)	
ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	
Знать:	
- методы анализа и оценки защищённости компьютерных систем - этапы и процедуры аудита информационной безопасности защищённых компьютерных систем	
Уметь:	
- разрабатывать различные методики оценки защищённости программно-аппаратных средств защиты информации компьютерных систем - применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации компьютерных систем - проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых компьютерных систем	
Владеть:	
- способами оценки защищённости компьютерных систем - методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых компьютерных систем нормативным требованиям по защите информации - способами контроля эффективности реализации политики информационной безопасности организации	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.27 Основы информационной безопасности
2	Б1.О.33 Программно-аппаратные средства защиты информации
3	Б1.О.31 Защита информации от утечки по техническим каналам
4	Б1.О.32 Основы управления информационной безопасностью
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.02 Комплексное обеспечение защиты информации объекта информатизации
2	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях
3	Б1.О.30 Моделирование систем защиты информации

4. Структура и содержание дисциплины

4.1. Очная форма обучения, 4 года (всего 180 часов, из них 84 часов аудиторных)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 4, Семестр 7					
Модуль 1: Теоретические основы аудита информационной безопасности					
1.1	<u>Лекция 1. Цели и задачи</u> Сущность и принципы управления аудитом ИБ. Цели и задачи системы управления аудитом. Основные понятия и терминология	Лек.	6	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.3
1.2	<u>Лекция 2. Основные этапы аудита безопасности</u> Этапы, процедуры аудита информационной безопасности защищённых компьютерных систем и организаций	Лек.	4	ОПК-1.4	Л2.1
1.3	<u>Лекция 3. Управление аудитом информационной безопасности</u> Концепция управления аудитом ИБ. Структура системы управления аудитом. Планирование аудиторской деятельности. Организация процесса аудита. Методология управления	Лек.	4	ОПК-1.4	Л1.1 Л1.2
1.4	<u>Лекция 4. Стандартизация и нормативное обеспечение аудита</u> Международные стандарты аудита информационной безопасности. Российские стандарты аудита информационной безопасности	Лек.	8	ОПК-1.4	Л1.1 Л1.2 Л2.3
1.5	Лабораторная работа 1. Оценка информационных рисков организации	ЛР	6	ОПК-1.4	Л1.1 Л1.2
1.6	Лабораторная работа 2. Анализ уязвимостей сетевой инфраструктуры	ЛР	6	ОПК-1.4	Л1.1 Л1.2
1.7	Лабораторная работа 3. Аудит систем аутентификации и управления доступом	ЛР	4	ОПК-1.4	Л1.1 Л1.2
1.8	Лабораторная работа 4. Мониторинг и анализ событий безопасности	ЛР	4	ОПК-1.4	Л1.1 Л2.1
1.9	Лабораторная работа 5. Тестирование на проникновение	ЛР	8	ОПК-1.4	Л1.1 Л1.3
1.10	Лабораторная работа 6. Комплексный аудит информационной безопасности	ЛР	6	ОПК-1.4	Л1.1 Л1.2
1.11	Современные подходы к организации аудита. Международные практики в области риск-менеджмента. Методы тестирования на проникновение. Анализ результатов тестирования осведомленности. Проверка соответствия систем защиты информации нормативным требованиям	СРС	10	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3
Модуль 2: Процессный подход к управлению аудитом информационной безопасности					
2.1	<u>Лекция 5. Классификация угроз</u> Модели угроз безопасности и уязвимостей информационных ресурсов	Лек.	4	ОПК-1.4	Л1.1 Л1.2 Л1.3
2.2	<u>Лекция 6. Методы оценки в аудите ИБ</u>	Лек.	4	ОПК-	Л2.2

	Методы оценки информационной безопасности защищённых автоматизированных систем и организаций			1.4	
2.3	Лекция 7. Сертификация результатов аудита ИБ Программа сертификации Интернет-сайтов и информационных систем	Лек.	4	ОПК-1.4	Л1.1 Л1.3
2.4	Практическая работа 1. Разработка политики информационной безопасности организации	ПЗ	4	ОПК-1.4	Л1.1 Л1.2
2.5	Практическая работа 2. Применение инструментов анализа защищённости	ПЗ	4	ОПК-1.4	Л1.1 Л1.3
2.6	Практическая работа 3. Организация системы мониторинга безопасности	ПЗ	4	ОПК-1.4	Л1.1 Л1.3
2.7	Практическая работа 4. Проведение аудита соответствия требованиям	ПЗ	4	ОПК-1.4	Л1.1 Л1.2
2.8	Аудит процессов реагирования на инциденты. Проверка соответствия криптографических решений стандартам. Аудит сетевой безопасности. Оценка безопасности жизненного цикла ПО. Проверка соблюдения правил ИБ сотрудниками	СРС	25	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3
Модуль 3: Курсовое проектирование					
3.1	Методы и инструменты аудита безопасности компьютерных систем	СРС	25	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3
Экзамен			36	ОПК-1.4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л3.1
Итого			180		

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	Подольский В.И., Щербакова Н.С., Комиссаров В.Л.	Компьютерные информационные системы в аудите	Москва: ЮНИТИ-ДАНА, 2023.	Э1
Л1.2	Гулак М.Л., Рытов М.Ю., Голембиовская О.М.	Аудит информационной безопасности. Прикладная статистика: учебное пособие	Москва: Ай Пи Ар Медиа, 2020	Э2
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Аверченков В.И.	Аудит информационной безопасности: учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012	Э3
Л2.2	Макаренко С.И.	Аудит безопасности критической	Санкт-Петербург:	Э4

		инфраструктуры специальными информационными воздействиями: монография	Научное издание, 2018	
Л2.3	Ситнов А.А.	Аудит информационной инфраструктуры: учебное пособие	Санкт-Петербург: Лань, 2011	Э5
5.1.3 Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Киреева Н. В., Поздняк И. С., Караулова О. А.	Аудит информационной безопасности: методические указания к практическим занятиям	Самара: ПГУТИ, 2019	Э6
5.2 Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/142668.html			
Э2	https://www.iprbookshop.ru/97630.html			
Э3	https://www.iprbookshop.ru/6991.html			
Э4	https://www.iprbookshop.ru/130084.html			
Э5	https://www.iprbookshop.ru/10615.html			
Э6	https://e.lanbook.com/book/223223			
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	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3 Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			

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
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, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.О.36.05 Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УВР _____
«__» _____ 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» ста-

		вится 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:		
Методы анализа и оценки защищённости компьютерных систем	Контрольная работа 1	Модуль 1 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
Этапы и процедуры аудита информационной безопасности защищённых компьютерных систем	Контрольная работа 2	Модуль 2 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
Уметь:		
Применять различные методики оценки защищённости программно-аппаратных средств защиты информации компьютерных систем	Лабораторная работа 1 Лабораторная работа 5	Модуль 1 0–5 за каждую работу «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Применять национальные и международные стандарты в области защиты информации для оценки защищённости компьютерных систем	Лабораторная работа 2 Лабораторная работа 3	Модуль 1 0–5 за каждую работу «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых компьютерных систем	Практическая работа 3 Практическая работа 4	Модуль 1 0–10 за каждую работу «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10

Владеть:		
Методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых компьютерных систем нормативным требованиям по защите информации	Лабораторная работа 4 Лабораторная работа 6	Модуль 1 0–5 за каждую работу «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Способами контроля эффективности реализации политики информационной безопасности организации	Практическая работа 1	Модуль 2 0–10 за каждую работу «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
Способами оценки защищённости компьютерных систем	Практическая работа 2	Модуль 2 0–10 за каждую работу «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
	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 текущего для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 4 лекционных занятия, 6 лабораторных работ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные практические занятия и лабораторные работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ОПК-1.4):

1. Основные задачи государственной системы ИБ.
2. Понятия внешнего и внутреннего аудита ИБ.
3. Основные услуги аудита информационной безопасности.
4. Цели и назначение проведения аудита информационной безопасности.
5. Основные типы аудита ИБ.
6. Основные этапы аудита.
7. Базовые факторы, способствующие повышению уязвимости информации.
8. Основные разделы отчета по результатам аудита безопасности ИС.
9. Рейтинг защищаемых ресурсов ИС.
10. Базовые задачи и этапы комплексного аудита ИБ систем.
11. Цели проведения аудита информационной безопасности.

12. Особенности сетевого аудита.
13. Организационные вопросы, решаемые на этапе инициирования процедуры аудита.
14. Базовые виды угроз информационной безопасности.
15. Основные этапы аудита безопасности внешнего периметра сети.
16. Основные виды аудита.
17. Базовые результаты экспертного аудита.
18. Основные методы тестирования ИС.
19. Общая характеристика сетевого сканера XSpider.
20. Основные компоненты стандарта COBIT.
21. Базовые этапы проведения аудита при использовании стандарта COBIT.
22. Общая характеристика сетевого сканера Сканер-ВС.

Лабораторная работа №1. Оценка информационных рисков организации.

Контрольные вопросы (ОПК-1.4):

1. Что такое информационные риски и как они влияют на безопасность организации?
2. Какие этапы включает в себя процесс оценки информационных рисков?
3. Как вы определяете уязвимости в информационных системах организации?
4. Какие методы оценки рисков (количественные и качественные) вы можете использовать и в каких случаях?
5. Каковы потенциальные последствия реализации рисков для бизнеса?
6. Какие стратегии можно использовать для управления и снижения информационных рисков в организации?

Лабораторная работа №2. Анализ уязвимостей сетевой инфраструктуры.

Контрольные вопросы (ОПК-1.4):

1. Что такое уязвимость сети и как она может повлиять на безопасность организации?
2. Какие методы и инструменты используются для анализа уязвимостей сетевой инфраструктуры?
3. Какова роль сканирования уязвимостей в процессе обеспечения сетевой безопасности?
4. Какие наиболее распространенные уязвимости могут быть обнаружены в сетевых устройствах?
5. Как проводить оценку риска, связанного с выявленными уязвимостями в сети?
6. Какие меры можно предпринять для устранения или снижения уязвимостей в сетевой инфраструктуре?

Лабораторная работа №3. Аудит систем аутентификации и управления доступом.

Контрольные вопросы (ОПК-1.4):

1. Что такое система аутентификации и какую роль она играет в обеспечении безопасности информации?
2. Какие методы аутентификации существуют и как они отличаются друг от друга?
3. Каковы основные критерии, по которым оценивается эффективность системы управления доступом?
4. Какие шаги включает в себя процесс аудита систем аутентификации и управления доступом?
5. Каковы потенциальные уязвимости в системах аутентификации и как можно их предотвратить?
6. Как проводить анализ логов аутентификации и доступа для выявления подозрительной активности?

Лабораторная работа №4. Мониторинг и анализ событий безопасности.

Контрольные вопросы (ОПК-1.4):

1. Какие основные типы событий безопасности могут быть зарегистрированы в системе?
2. Каковы ключевые элементы эффективной стратегии мониторинга безопасности?
3. Что такое корреляция событий безопасности и почему она важна для анализа?
4. Какие инструменты или средства можно использовать для мониторинга событий безопасности?
5. Какова роль SIEM в мониторинге безопасности?
6. Какую информацию необходимо учитывать при оценке инцидента безопасности?

Лабораторная работа №5. Тестирование на проникновение.

Контрольные вопросы (ОПК-1.4):

1. Какие этапы включает в себя процесс тестирования на проникновение?
2. Каковы основные цели тестирования на проникновение?
3. Что такое активное и пассивное тестирование на проникновение, и в чем между ними разница?
4. Какие инструменты обычно используются для проведения тестирования на проникновение?
5. Каковы юридические и этические аспекты, которые необходимо учитывать при тестировании на проникновение?
6. Как правильно документировать результаты тестирования на проникновение для дальнейшего анализа и исправления уязвимостей?

Лабораторная работа №6. Комплексный аудит информационной безопасности.

Контрольные вопросы (ОПК-1.4):

1. Что такое комплексный аудит информационной безопасности и какие его основные цели?
2. Какие ключевые компоненты должны быть включены в аудит информационной безопасности?
3. Какова роль стандартов и нормативных документов в проведении аудита информационной безопасности?
4. Какие методы и инструменты могут быть использованы для оценки уровня информационной безопасности в организации?
5. Как осуществляется анализ выявленных уязвимостей и рисков в процессе аудита?
6. Как правильно составить отчет о результатах аудита информационной безопасности и что в него должно входить?

Модуль 2 (50 баллов):

Модуль содержит 3 лекционных, 4 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные практические занятия и лабораторные работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы 2 (ОПК-1.4):

1. Структура стандарта BS7799.
2. Анализ уровня защищённости интернет-сайтов с помощью GIAC.

3. Структура немецкого стандарта BSI/IT.
4. Общая характеристика семейства международных стандартов ISO/IEC 27000.
5. Необходимость аудита ИБ.
6. Виды аудита ИБ.
7. Критерии аудита ИБ.
8. Принципы аудита ИБ.
9. Роли при проведении аудита ИБ.
10. Сбор свидетельств аудита ИБ.
11. Анализ свидетельств аудита ИБ.
12. Завершение аудита ИБ.
13. Отчёт и заключение по результатам аудита ИБ.
14. Оценка соответствия ИБ автоматизированных организаций требованиям нормативных документов по ИБ.
15. Процессноориентированная оценка ИБ объекта.
16. Рискоориентированная оценка ИБ объекта.
17. Планирование программы аудита ИБ.
18. Реализация и поддержка программы аудита ИБ.
19. Контроль и совершенствование программы аудита ИБ.
20. Корпоративные стандарты и руководства в области аудита и оценки ИБ. Стандарты Банка России
21. Планирование аудита, его назначение и принципы.
22. Разработка предварительного и общего плана аудита, аудиторской программы и конкретных аудиторских
23. процедур.
24. Существенность в аудите.
25. Аудиторский риск. Виды риска.
26. Изучение и оценка систем бухгалтерского учета и внутреннего контроля в ходе аудита.
27. Взаимодействие аудиторской организации с проверяемой организацией
28. Модель измерения и оценивания информационной безопасности
29. Модель проведения оценки информационной безопасности
30. Измерение атрибутов объекта оценки ИБ с помощью анкет
31. Измерение атрибутов объекта оценки ИБ с помощью метрик
32. Оценка информационной безопасности на основе оценки процессов.

Практическое занятие №1. Разработка политики информационной безопасности организации.

Контрольные вопросы (ОПК-1.4):

1. Какие основные элементы должны быть включены в политику информационной безопасности организации?
2. Каковы ключевые цели и задачи политики информационной безопасности?
3. Как проводится оценка рисков для определения необходимых мер в политике информационной безопасности?
4. Какова роль заинтересованных сторон в процессе разработки политики информационной безопасности?
5. Какие шаги необходимо предпринять для успешной реализации и распространения политики среди сотрудников?
6. Как регулярно обновлять и пересматривать политику информационной безопасности в ответ на изменяющиеся угрозы и технологии?

Практическое занятие №2. Применение инструментов анализа защищённости.

Контрольные вопросы (ОПК-1.4):

1. Какие основные категории инструментов анализа защищённости существуют и чем они отличаются друг от друга?

2. Каковы ключевые функции сканеров уязвимостей в процессе анализа защищённости?
3. Как проводить оценку защищённости сети с использованием инструментов анализа?
4. Каковы преимущества и недостатки использования автоматизированных инструментов анализа защищённости?
5. Как интерпретировать результаты анализа защищённости для принятия управленческих решений?
6. Как можно комбинировать различные инструменты анализа защищённости для построения более надёжной системы защиты?

Практическое занятие №3. Организация системы мониторинга безопасности.

Контрольные вопросы (ОПК-1.4):

1. Какие основные компоненты входят в систему мониторинга безопасности?
2. Каковы основные цели и задачи организации системы мониторинга безопасности?
3. Какие технологии и инструменты используются для сбора и анализа данных о безопасности?
4. Как осуществляется интеграция системы мониторинга с существующими ИТ-инфраструктурами?
5. Каковы методы защиты данных, собираемых системой мониторинга безопасности?
6. Какие критерии оценки эффективности системы мониторинга безопасности можно использовать?

Практическое занятие №4. Проведение аудита соответствия требованиям.

Контрольные вопросы (ОПК-1.4):

1. Какие основные этапы включает в себя процесс аудита соответствия требованиям?
2. Каковы ключевые документы, которые необходимо подготовить перед проведением аудита?
3. Какие методы и подходы используются для оценки соответствия требованиям?
4. Каковы основные критерии, по которым оценивается эффективность проведенного аудита?
5. Какие действия необходимо предпринять в случае выявления несоответствий в ходе аудита?
6. Роли аудиторов в процессе проведения аудита соответствия требованиям.

1.3.2 Модуль: «Курсовая работа» (100 баллов):

Тема курсовой работы:

«Методы и инструменты аудита безопасности компьютерных систем».

Для выполнения курсовой работы обучающиеся получают индивидуальное задание, включающее в себя исходные данные компьютерной системы типичной организации, на примере которой необходимо провести аудит информационной безопасности.

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 ОПК-1.4 и ПК-3 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, для аудита было рассмотрено несколько методов, описаны преимущества и недостатки каждого из них. - задание выполнено в полном объеме, один или несколько рассматриваемых вопросов раскрыты неполно, для аудита был определен изначально один метод. - один или несколько пунктов задания не выполнены или выполнены не в полном объеме	20 10 0
2.	Применение инструментальных средств: - для аудита была определена методика, был проведен обзор популярных инструментов, указаны для каких целей применяется каждый инструмент и в чем его особенности, определена методика аудита. - для аудита была определена методика, проведен обзор популярных инструментов, однако не указано для каких целей применяется каждый инструмент и в чем его особенности. - для аудита была определена методика, использовался ограниченный набор инструментов без обоснования их применения; - определенная методика аудита и инструментарий не отражает основных этапов аудита.	20 14 8 2
3.	Оформление результатов работы - курсовой проект оформлен в полном соответствии с ЕСКД; - курсовой проект оформлен с незначительными отклонениями от ЕСКД; - оформление проекта 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 0 до 40 баллов получает по курсовой работе оценку «неудовлетворительно». Обучающийся, набравший от 41 до 60 баллов – «удовлетворительно», от 61 до 80 баллов – «хорошо», от 81 до 100 баллов – «отлично».

1.3.3 Вопросы, выносимые на экзамен по дисциплине (ОПК-1.4) (промежуточная аттестация):

1. Основные задачи государственной системы ИБ.
2. Понятия внешнего и внутреннего аудита ИБ.
3. Основные услуги аудита информационной безопасности.
4. Цели и назначение проведения аудита информационной безопасности.
5. Основные типы аудита ИБ.
6. Основные этапы аудита.
7. Базовые факторы, способствующие повышению уязвимости информации.
8. Основные разделы отчета по результатам аудита безопасности ИС.
9. Рейтинг защищаемых ресурсов ИС.
10. Базовые задачи и этапы комплексного аудита ИБ систем.
11. Цели проведения аудита информационной безопасности.

12. Особенности сетевого аудита.
13. Организационные вопросы, решаемые на этапе инициирования процедуры аудита.
14. Базовые виды угроз информационной безопасности.
15. Основные этапы аудита безопасности внешнего периметра сети.
16. Основные виды аудита.
17. Базовые результаты экспертного аудита.
18. Основные методы тестирования ИС.
19. Общая характеристика сетевого сканера XSpider.
20. Основные компоненты стандарта COBIT.
21. Базовые этапы проведения аудита при использовании стандарта COBIT.
22. Общая характеристика сетевого сканера Сканер-ВС.
23. Структура стандарта BS7799.
24. Анализ уровня защищённости интернет-сайтов с помощью GIAC.
25. Структура немецкого стандарта BSI/IT.
26. Общая характеристика семейства международных стандартов ISO/IEC 27000.
27. Необходимость аудита ИБ.
28. Виды аудита ИБ.
29. Критерии аудита ИБ.
30. Принципы аудита ИБ.
31. Роли при проведении аудита ИБ.
32. Сбор свидетельств аудита ИБ.
33. Анализ свидетельств аудита ИБ.
34. Завершение аудита ИБ.
35. Отчёт и заключение по результатам аудита ИБ.
36. Оценка соответствия ИБ автоматизированных организаций требованиям нормативных документов по ИБ.
37. Процессноориентированная оценка ИБ объекта.
38. Рискоориентированная оценка ИБ объекта.
39. Планирование программы аудита ИБ.
40. Реализация и поддержка программы аудита ИБ.
41. Контроль и совершенствование программы аудита ИБ.
42. Корпоративные стандарты и руководства в области аудита и оценки ИБ. Стандарты Банка России
43. Планирование аудита, его назначение и принципы.
44. Разработка предварительного и общего плана аудита, аудиторской программы и конкретных аудиторских
45. процедур.
46. Существенность в аудите.
47. Аудиторский риск. Виды риска.
48. Изучение и оценка систем бухгалтерского учета и внутреннего контроля в ходе аудита.
49. Взаимодействие аудиторской организации с проверяемой организацией
50. Модель измерения и оценивания информационной безопасности
51. Модель проведения оценки информационной безопасности
52. Измерение атрибутов объекта оценки ИБ с помощью анкет
53. Измерение атрибутов объекта оценки ИБ с помощью метрик
54. Оценка информационной безопасности на основе оценки процессов.

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

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 обучающимся 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 блокам модулей дисциплины

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	20	30
Модуль 2	50	10	40
Модуль - КР	100	40	60
Экзамен	100	100	

Как правило, 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. Рекомендуются формировать вопросы в экзаменационных 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 ФЕДЕРА- ЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИБ» _____ Д.В. Маршаков « ____ » _____ 20 ____ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 3 Дисциплина: Методы оценки безопасности компьютерных систем (Аудит компьютерных си- стем)		
Билет №1 1. Цели и назначение проведения аудита информационной безопасности. 2. Аудиторский риск. Виды риска. Доцент каф. «ИБ» _____ Маршаков Д.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 по дисциплине «Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)»

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-1.4

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.

Ключи к ответам представлены в отдельной таблице.

ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

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	Риск является функцией... 1. размера возможного ущерба 2. числа пользователей информационной системы 3. уставного капитала организации 4. территориального размера организации
2	Целью проведения анализа рисков НЕ является... 1. Делегирование полномочий 2. Количественная оценка воздействия потенциальных угроз 3. Выявление рисков 4. Определение баланса между воздействием риска и стоимостью необходимых контрмер
3	Политика безопасности строится на основе... 1. общих представлений об ИС организации 2. изучения политик родственных организаций 3. анализа рисков 4. готовых шаблонов
4	Управление рисками включает в себя следующие виды деятельности: 1. определение ответственных за анализ рисков 2. оценка рисков 3. выбор эффективных защитных средств
5	Задачей руководства в процессе внедрения и сопровождения безопасности НЕ является 1. Поддержка 2. Выполнение анализа рисков 3. Определение цели и границ 4. Делегирование полномочий
6	Остаточный риск рассчитывается - как 1. Угрозы x Риски x Ценность актива 2. (Угрозы x Ценность актива x Уязвимости) x Риски 3. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля 4. Угрозы x Ценность актива x Недостаток контроля

№ задания	Тексты заданий
7	В число этапов управления рисками входят: +1. идентификация активов 2. ликвидация пассивов +3. выбор объектов оценки 4. диверсификация
8	Искусственные угрозы безопасности информации вызваны: 1. деятельностью человека 2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения 3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека 4. корыстными устремлениями злоумышленников 5. ошибками при действиях персонала
9	К внутренним нарушителям информационной безопасности относится... 1. клиенты 2. пользователи системы 3. посетители 4. любые лица, находящиеся внутри контролируемой территории 5. технический персонал, обслуживающий здание
10	К посторонним лицам нарушителям информационной безопасности относится... 1. персонал, обслуживающий технические средства 2. технический персонал, обслуживающий здание 3. пользователи 4. представители конкурирующих организаций 5. лица, нарушившие пропускной режим

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

№ задания	Тексты заданий
11	Восстановите соответствие. 1. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам 2. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных 3. Государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных А. обладатель информации Б. оператор информационной системы В. субъект персональных данных
12	Восстановите соответствие каналов распространения информации и их содержимого. 1. средства массовой информации 2. средства передачи официальной информации 3. конференции 4. обмен официальными документами А. неформальные Б. формальные В. неформальные Г. формальные
13	Восстановите соответствие средств взаимодействия с системой. 1. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе по сети Интернет 2. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом 3. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации

№ задания	Тексты заданий
	А. Шифрование Б. Авторизация В. Аутентификация.
14	Восстановите соответствие уровней защиты информации 1. административный уровень 2. программно-технический уровень 3. процедурный уровень А. Представляет собой комплекс мер, применяемых руководством организации Б. Уровень, на котором находятся непосредственно средства защиты В. Состоит из мер, реализуемых людьми

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Восстановите последовательность действий организации аттестации выделенного помещения по требованиям безопасности информации 1. Подготовительный этап 2. Проведение аудита помещения 3. Подготовка документации и сопутствующих материалов проведенного аудита
16	Восстановите последовательность подготовительного этапа аудита безопасности: 1. Определение вида аудита 2. Согласование целей, задач и объема работ 3. Составление регламента проведения аудита 4. Определение используемых методик и инструментов 5. Установление сроков и стоимости работ
17	Последовательность проведения аудита информационной безопасности 1. Выбор методик и инструментов 2. Анализ документации и изучение инфраструктуры 3. Оценка мер защиты и выявление уязвимостей 4. Оценка рисков 5. Формирование результатов

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	В число основных принципов архитектурной безопасности входят _____
19	К организационно - административному обеспечению информации относится: _____
20	Основопологающие документы для обеспечения безопасности внутри организации: _____

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 3 баллами; если допущена одна ошибка/неточность/ответ правильный, но не полный - 1 балл, если допущено более одной ошибки/ответ неправильный/ ответ отсутствует- 0 баллов.

Ключи к тестовым заданиям по оценке компетенции ОПК-1.4

№ задания	Верный ответ			
1	1			
2	1			
3	3			
4	2,3			
5	2			
6	3			
7	1,3			
8	1			
9	5			
10	4			
11	1	2		3
	А	Б		В
12	1	2	3	4
	А	Б	В	Г
13	1	2		3
	А	Б		В
14	1	2		3
	А	Б		В
15	1, 2, 3			
16	1, 2, 3, 4, 5			
17	1, 2, 3, 4, 5			
18	- усиление самого слабого звена, - эшелонированность обороны			
19	- взаимоотношения исполнителей, - подбор персонала, - регламентация производственной деятельности			
20	- трудовой договор сотрудников, - должностные обязанности руководителей, - коллективный договор			

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, необхо-

димо 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.

Для подготовки и выполнения практических занятий используется учебно-методическое пособие: *Киреева Н.В. Аудит информационной безопасности : методические указания* / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223223> (дата обращения: 17.08.2025). — Режим доступа: для авториз. пользователей.

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 практических занятий используется учебно-методическое пособие: *Киреева Н.В. Аудит информационной безопасности : методические указания* / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223223> (дата обращения: 17.08.2025). — Режим доступа: для авториз. пользователей.

3. Методические указания для обучающихся по подготовке курсовой работы

В ходе выполнения курсовой работы обучающийся решает следующие задачи:

1. Рассматривает основные методы аудита, такие как анализ уязвимостей, социальная инженерия, тестирование на проникновение, оценка политик и процедур безопасности, сравнить плюсы и минусы различных методов.
2. Выполняет обзор инструментов аудита безопасности, исследует популярные инструменты для аудита безопасности, оценивает их функциональные возможности и применимость.
3. Выполнить аудит безопасности на примере заданной компьютерной системы или сети, документирует процесс и полученные результаты.
4. Проводит оценка результата аудита, дает рекомендации и заключения

Порядок выполнения курсовой работы приведен в методических материалах по ее выполнению. Критерии оценки курсовой работы приведены в оценочных материалах дисциплины.

4. 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 обучающегося имеет существенное значение.

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

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

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.

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

Дополнительные самостоятельные исследования в лаборатории. Обучающиеся, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные

исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения обучающихся в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы обучающимся во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

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

Методику самостоятельной работы все обучаемые выбирают индивидуально.

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