МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ Н.А. Андреева
«29» 04 2024 г.

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

рабочая программа дисциплины

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

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

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

Программу составил:
Доцент кафедры ИВТ, к.т.н., доцент Чикалов А.Н.

Рецензенты:
Ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи»,
д.т.н., доцент Погорелов В.А.

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

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

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

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

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

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

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

"Информационная безопасность"

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

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

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

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

---

1. Цели изучения дисциплины

Целями изучения дисциплины **"Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)"** является: формирование компетенций по основным разделам данного курса, изучение студентами основных методов оценки безопасности компьютерных систем, стандартов в этой области, получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем, приобретение навыков применять современные методы оценки безопасности компьютерных систем.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-1.4: способен администрировать средства защиты информации в компьютерных системах и сетях
Знать:
- базовые понятия и принципы применения современных методов оценки безопасности компьютерных систем.
Уметь:
- выявлять угрозы и определять их актуальность для современных компьютерных систем; - описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем.
Владеть:
- практическими навыками применения методов обеспечения безопасности компьютерных систем.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.31 Защита информации от утечки по техническим каналам
2	Б1.В.03 Защита информации от вредоносного программного обеспечения
3	Б1.О.29 Методы и средства криптографической защиты информации
4	Б1.О.30 Программно-аппаратные средства защиты информации
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях
2	Б1.О.33 Комплексное обеспечение защиты информации объекта информатизации
3	Б1.В.09 Аналитика DLP-систем

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

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 84 аудиторных часов, 60 часов самостоятельной работы)

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: Общие вопросы оценки безопасности компьютерных систем					
1.1	Лекция 1. Введение. Основные понятия курса. Модель нарушителя. Организационно-правовые вопросы защиты информации.	Лек.	6	ОПК-1.4	Л1.1, Л1.2, Л2.1
1.2	Основные понятия курса. Модель нарушителя. Организационно-правовые вопросы защиты информации.	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.1
1.3	Лекция 2. : «Защита информации от ПЭМИН» Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	Лек.	2	ОПК-1.4	Л1.1, Л1.2, Л2.1
1.4	Защита информации от ПЭМИН	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.1
1.5	Лекция 3. «Основы криптографии» Понятия и определения; классификация шифров; блочные и поточные шифры.	Лек.	6	ОПК-1.4	Л1.1, Л1.2, Л2.1
1.6	Основы криптографии Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности.	СРС	2	ОПК-1.4	Л1.1, Л2.2, Л2.1, Л3.3
1.7	Практическое занятие 1. Оценка технологической безопасности программного продукта.	Пр.	4	ОПК-1.4	Л1.1, Л1.2, Л2.1 Л3.2
1.8	Специфические особенности защиты информации в компьютерных сетях. Методы и средства защиты информационно-программного обеспечения на уровне операционных систем	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.1 Л3.1
1.9	Применение симметричных криптосистем для защиты компьютерной информации.	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.1
1.10	Практическое занятие 2. Оценка безопасности информационной системы по критериям СТСРЕС. Оценки пригодности компьютерных систем TCSEC (Оранжевая книга).	Пр.	6	ОПК-1.4	Л1.1, Л1.2, Л2.2, Л3.2
1.11	Лабораторная работа 1. Модель нарушителя. Организационно-правовые вопросы защиты информации.	Лаб.	12	ОПК-1.4	Л1.1, Л1.2, Л3.1
1.12	Лекция 4. «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности» Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии	Лек.	4	ОПК-1.4	Л1.1, Л1.2, Л2.1

	безопасности информационных технологий.				
1.13	Технологии идентификации и аутентификации в компьютерных сетях.	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л3.1
1.14	Лабораторная работа 2. Защита информации от ПЭМИН. Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	Л.р.	12	ОПК-1.4	Л1.1, Л1.2, Л3.1
Модуль 2: Организация оценки безопасности компьютерных систем					
2.1	Лекция 5. «Специфические особенности защиты информации в компьютерных сетях» Разделение совместно используемых ресурсов. Расширение зоны контроля. Комбинация различных программно-аппаратных средств. Неизвестный периметр. Множество точек атаки. Сложность управления и контроля доступа к системе. Средства защиты информации от НСД. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах.	Лек.	6	ОПК-1.4	Л1.1, Л1.2, Л2.1, Л2.2
2.2	Методы защиты внешнего периметра компьютерных сетей. Безопасность компьютерных систем	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.1, Л2.2
2.3	Методы обеспечения информационной безопасности .	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.1
2.4	Эксплуатация уязвимостей.	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л3.1
2.5	Лекция 6. «Методы и средства защиты информационно-программного обеспечения на уровне операционных систем». Классы защищенности СВТ от НСД. Требования безопасности информации к операционным системам. Профили защиты операционных систем. Разграничение полномочий для групп и учетных записей пользователей. Локальная групповая политика	Лек.	6	ОПК-1.4	Л1.1, Л1.2, Л2.2, Л2.3
2.6	Основы технологии виртуальных защищенных сетей VPN.	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.2, Л2.3
2.7	Мероприятия по выявлению каналов утечки информации	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.3, Л2.4
2.8	Технологии обнаружения вторжений в компьютерных сетях.	СРС	2	ОПК-1.4	Л1.1 Л1.2 Л2.4
2.9	Лабораторная работа 3. Классификация шифров. Блочные и поточные шифры.	Л.р.	10	ОПК-1.4	Л1.1, Л1.2, Л3.1
2.10	Методы идентификации и аутентификации пользователей компьютерных систем.	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л3.2

2.11	Адаптивное управление безопасностью в компьютерных сетях	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л2.2
2.12	Особенности современных подходов к анализу информационной безопасности. Анализ методов функционирования современного Вредоносного программного обеспечения. Способы определения нарушений информационной безопасности. Программно-конфигурируемые сети	СРС	2	ОПК-1.4	Л1.1, Л1.2, Л3.1
2.13	Практическое занятие 3. Оценка безопасности информационной системы по общим критериям	Пр.	6	ОПК-1.4	Л1.1, Л1.2, Л3.6
	Курсовая работа	СРС	30	ОПК-1.4	Л1.1, Л1.2, Л2.1, Л2.2 Л2.3, Л2.4 Л3.1, Л3.2 Л3.3, Л3.4 Л3.5 Л3.6
	Экзамен		**36**		
	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	Милославская Н.Г., Сенаторов И.Ю., Толстой А.И.	Технические, организационные и кадровые аспекты управления информационной безопасностью	М.: Горячая линия –Телеком, 2014 г.- 154 с.	20
Л1.2	Милославская Н.Г., Сенаторов И.Ю., Толстой А.И.	Проверка и оценка деятельности по управлению информационной безопасностью	М.: Горячая линия –Телеком, 2014 г.- 123 с.	20
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Малюк А.А., Горбатов В.С., и др.	Введение в информационную безопасность	М.: Горячая линия-Телеком, 2011. - 436с	10
Л2.2	Алферов А.П., Зубов А.Ю., и др.	Основы криптографии	М.:Гелиос АРВ, 2002 г. -367 с.	3

Л2.3	Ярочкин В.И.	Информационная безопасность	М.: Академический проект, 2003. – 425 с.	3
Л2.4	Девянин П.Н.	Модели безопасности компьютерных систем	М.: Горячая линия-Телеком, 2011. - 383с	5
5.1.3 Методическое обеспечение для самостоятельной работы обучающихся				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Мельников В.В.	Защита информации в компьютерных системах	М.: Финансы и статистика, 2014. – 368 с.	Э2
Л3.2	Романец Ю.В.	Защита информации в компьютерных системах и сетях	М.: Радио и связь, 2001. – 328 с.	Э4
Л3.3	Иванов М.А.	Криптографические методы защиты информации в компьютерных системах и сетях	М.: Электрон «Кудиц образ», 2001. – 386 с.	Э3
Л3.4	Руководящий документ Гостехкомиссии России	Средства вычислительной техники	М.: ГТК РФ, 1992..	Э5
Л3.5	Герасименко В.А.	Защита информации в автоматизированных системах обработки данных	М.: Энергоавтомиздат. 2016 г.	Э1
Л3.6	Червяков Н.И., Бабенко М.Г., Гладков А.В.	Вероятностные методы оценки состояния информационной безопасности: учебное пособие	Ставрополь: Северо-Кавказский Федеральный Университет. 2017. – 182 с., СКФ МТУСИ, 2016 г.	Э6
5.2 Электронные образовательные ресурсы				
Э1	http://www.iprbookshop.ru/73733/html			
Э2	http://www.iprbookshop.ru/61558/html			
Э3	http://www.iprbookshop.ru/24451/html			
Э4	http://www.iprbookshop.ru/29257/html			
Э5	http://www.iprbookshop.ru/73733/html			
Э6	http://www.iprbookshop.ru/92536/html			
5.3 Программное обеспечение				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
П.3	Kaspersky Endpoint Security (лицензия)			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интер-

	нет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

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

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

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

Существенное значение имеет самостоятельная работа студента.

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

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

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

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

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

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

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное по-

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

Использование Интернет-ресурсов

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

Рекомендации по подготовке к рубежным аттестациям

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

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

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

Подготовка к экзамену осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к экзамену необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, кото-

рые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

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

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

Дополнения и изменения в Рабочей программе