Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Методы оценки безопасности компьютерных систем
наименование дисциплины по ОПОП

для специальности 10.05.03 Информационная безопасность автоматизированных систем
код и полное наименование специальности

по специализации Безопасность открытых информационных систем

факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 5 семестр (ы) 9
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем с учетом рекомендаций и ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

Разработчик _____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«17» 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)_____
_____ Качаева Г.И.,к.э.н._____
подпись (ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 20 сентября 2021 года, протокол № 2 .

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)
_____ Качаева Г.И., к.э.н._____
подпись (ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от «18» октября 2021 г., протокол № 2

Председатель Методического совета факультета КТВТиЭ
_____ Исабекова Т.И., к.ф-м.н., доцент
подпись (ФИО уч. степень, уч. звание)

от «18» октября 2021 г.

Декан факультета _____ Юсуфов Ш.А.
подпись ФИО

Начальник УО _____ Магомаева Э.В.
подпись ФИО

И.о проректора по УР _____ Баламирзоев Н.Л.
подпись ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) дисциплины «Методы оценки безопасности компьютерных систем» формирование у студентов знаний и умений в области теории и проблематики вопросов, связанных с современными методами анализа данных в системах информационной безопасности, технологиями интеллектуального анализа больших информационных массивов с помощью информационно-аналитических систем.

Задачами дисциплины являются: - изучение основных методов оценки защищенности компьютерных систем, стандартов в этой области; - получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем; - студенты должны научиться применять современные методы оценки защищенности компьютерных систем на практике.

2.Место дисциплины в структуре ОПОП

Дисциплина «Методы оценки безопасности компьютерных систем» относится к части, формируемой участниками образовательных отношений, дисциплины по выбору 3.

Предшествующими дисциплинами, формирующими начальные знания, являются: Гуманитарные аспекты информационной безопасности, Правоведение.

Последующими дисциплинами являются: Организационное и правовое обеспечение информационной безопасности, Производственная (научно-исследовательская работа) практика.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

В результате освоения дисциплины «Методы оценки безопасности компьютерных систем» студент должен овладеть следующими компетенциями: ПК-1.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ПК - 1	Способен проводить оценивание уровня безопасности компьютерных систем и сетей	ПК-1.З.1. ПК-11.З.1. Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации;
		ПК-1.У.2. Уметь: проводить анализ средств защиты с целью определения уровня обеспечиваемой ими защищенности и доверия.

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	5/180		
Семестр	9		
Лекции, час	34		
Практические занятия, час	-		
Лабораторные занятия, час	34		
Самостоятельная работа, час	76		
Курсовой проект (работа), РГР, семестр	-		
Зачет (при заочной форме **4 часа** отводится на контроль)	-		
Часы на экзамен (при очной, очно-заочной формах **1 ЗЕТ – 36 часов**, при заочной форме **9 часов** отводится на контроль)	**36**		

4.1.Содержание дисциплины (модуля) «Методы оценки безопасности компьютерных систем»

№ п/п	Раздел дисциплины, тема лекции и вопросы	Очная форма				Очно-заочная форма				Заочная форма			
		ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР
1	**Лекция №1 Тема: «Введение»** Основные понятия курса. Модель нарушителя. Организационно-правовыевопросызащитыинформации.	2	-	2	4								
2	**Лекция №2 Тема: «Защита информации от ПЭМИН»** Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	2		2	4								
3	**Лекция № 3 Тема: «Основы криптографии»** Понятия и определения; классификация шифров; блочные и поточные шифры.	2	-	2	4								
4	**Лекция №4 Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»** Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии безопасности информационных технологий.	2	-	2	4								
5	**Лекция № 5 Тема: «Специфические особенности защиты информации в компьютерных сетях»** Разделениесовместноиспользуемыхресурсов.Расширениезоныконтроля.Комбинацияразличныхпрограммно-аппаратныхсредств.Неизвестныйпериметр.Множествоточекатаки.Сложностьуправленияиконтролядоступаксистеме.Средствазащитыинформацииот НСД.Способынесанкционированногодоступакинформацииизащитыотнеговкомпьютерныхсистемах.	2	-	2	4								
6	**Лекция № 6 Тема: «Методы и средства защиты информационно-программного обеспечения на уровне операционных систем»** КлассызащищенностиСВТотНСД.Требованиябезопасностиинформациикоперационнымсистемам.Профилизащитыоперационных систем.Разграничениеполномочийдлягруппиучетныхзаписейпол	2	-	2	4								

	ьзователей.Локальнаягрупповаяполитика.												
7	**Лекция № 7 Тема: «Применение симметричных криптосистем для защиты компьютерной информации»** Поля Фейстеля; стандарт шифрования данных DES; отечественный стандарт шифрования данных.	2	-	2	4								
8	**Лекция № 8 Тема: «Технологии идентификации и аутентификации в компьютерных сетях»** Управлениедоступом.Сервисыбезопасности.	2	-	2	4								
9	**Лекция № 9 Тема: «Методы защиты внешнего периметра компьютерных сетей»** Фильтрыпакетов.Шлюзысеансовогоуровня.Шлюзыприкладного уровня.Межсетевыеэкраныэкспертногоуровня.Системыобнаружениявторжений.IDSуровнясети.IDSуровняхоста.	2	-	2	4								
10	**Лекция № 10 Тема: «Безопасность компьютерных систем»** Задачи информационной безопасности. Конфиденциальность, целостность, доступность данных и программ. Понятие политики безопасности.	2	-	2	6								
11	**Лекция № 11 Тема: «Методы обеспечения информационной безопасности»** Криптография, модели безопасности, контроль поведения.Программные уязвимости, виды уязвимостей.	2	-	2	6								
12	**Лекция № 12 Тема: «Эксплуатация уязвимостей»** Инструменты. Информация о процессах в системе.	2	-	2	4								
13	**Лекция № 13 Тема: «Основы технологии виртуальных защищенных сетей VPN»** ОсновытехнологииивиртуальныхзащищенныхсетейVPN.Технологиивиртуальныхзащищенныхсетей VPN.Концепцияпостроениявиртуальныхзащищенныхсетей VPN.Основныепонятиеифункциисети VPN.Методыреализациибезопасности VPN.	2	-	2	4								
14	**Лекция № 14 Тема: «Мероприятия по выявлению каналов утечки информации»** Специальные проверки. Порядок проведения специальной проверки технических средств.	2	-	2	6								
15	**Лекция № 15 Тема: «Технологии обнаружения вторжений в**	2	-	2	4								

	компьютерных сетях» Способсбораинформации.Методанализаинформации.Способреагированиянаугрозы.ТребованиякIDS.Использованиеуязвимостей.ТестированиесистемIDS.												
16	**Лекции № 16 Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»** Аутентификация данных; алгоритмы безопасного хеширования; ЭЦП криптосистем RSA и Эль Гамаля; алгоритм цифровой подписи DSA; отечественные алгоритмы цифрой подписи.	2	-	2	6								
17	**Лекция № 17 Тема: «Адаптивное управление безопасностью в компьютерных сетях»** Особенности современных подходов к анализу информационной безопасности. Анализ методов функционирования современного Вредоносного программного обеспечения. Способы определения нарушений информационной безопасности. Программно-конфигурируемые сети	2	-	2	4								
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 1-5 тема 2 аттестация 6-10 тема 3 аттестация 11-15 тема								Входная конт.работа; Контрольная работа			
Форма промежуточной аттестации (по семестрам)		Экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		**34**	**-**	**34**	**76**								

К видам учебной работы в вузе отнесены: лекции, консультации, семинары, практические занятия, лабораторные работы, контрольные работы, коллоквиумы, самостоятельные работы, научно- исследовательская работа, практики, курсовое проектирование (курсовая работа). Вуз может устанавливать другие виды учебных занятий.

** - Разделы, тематику и вопросы по дисциплине следует разделить на три текущие аттестации в соответствии со сроками проведения текущих аттестаций. По материалу программы, пройденному студентом после завершения 3-ей аттестации до конца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче зачета или экзамена.*

4.2. Содержание лабораторных (практических) занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Очно-заочно	Заочно	
1	2	3	4	5	6	7
1	№1	Модель нарушителя. Организационно-правовые вопросы защиты информации.	2			№№ 1-6
2	№2	Защита информации от ПЭМИН. Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	2			№№ 1-6
3	№3	Классификация шифров. Блочные и поточные шифры.	2			№№ 1-6
4	№ 4	Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности.	2			№№ 1-6
5	№5	Специфические особенности защиты информации в компьютерных сетях.	2			№№ 1-6
6	№6	Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.	2			№№ 1-6
7	№7	Применение симметричных криптосистем для защиты компьютерной информации.	2			№№ 1-6
8	№8	Технологии идентификации и аутентификации в компьютерных сетях.	2			№№ 1-6
9	№9	Методы защиты внешнего периметра компьютерных сетей.	2			№№ 1-6
10	№10	Безопасность компьютерных систем.	2			№№ 1-6
11	№11	Методы обеспечения информационной безопасности.	2			№№ 1-6
12	№12	Эксплуатация уязвимостей.	2			№№ 1-6
13	№13	Основы технологии виртуальных защищенных сетей VPN.	2			№№ 1-6
14	№14	Мероприятия по выявлению каналов утечки информации	2			№№ 1-6
15	№15	Технологии обнаружения вторжений в компьютерных сетях.	2			№№ 1-6

16	№16	Методы идентификации и аутентификации пользователей компьютерных систем.	2			№№ 1-6
17	№17	Адаптивное управление безопасностью в компьютерных сетях.	2			№№ 1-6
ИТОГО			**34**			

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		Очно	Очно-заочно	Заочно		
1	2	3	4	5	6	7
1	Основные понятия курса. Модель нарушителя. Организационно-правовыевопросызащитыинформации.	4			№№ 1-6	Опрос, реферат
2	Защита информации от ПЭМИН	4			№№ 1-6	Опрос, реферат
3	Основы криптографии	4			№№ 1-6	Опрос, реферат
4	Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности.	4			№№ 1-6	Опрос, реферат
5	Специфические особенности защиты информации в компьютерных сетях.	4			№№ 1-6	Опрос, реферат
6	Методы и средства защиты информационно-программного обеспечения на уровне операционных систем.	4			№№ 1-6	Опрос, реферат
7	Применение симметричных криптосистем для защиты компьютерной информации.	4			№№ 1-6	Опрос, реферат
8	Технологии идентификации и аутентификации в компьютерных сетях.	4			№№ 1-6	Опрос, реферат
9	Методы защиты внешнего периметра компьютерных сетей.	4			№№ 1-6	Опрос, реферат
10	Безопасность компьютерных систем.	6			№№ 1-6	Опрос, реферат
11	Методы обеспечения информационной безопасности.	6			№№ 1-6	Опрос, реферат
12	Эксплуатация уязвимостей.	4			№№ 1-6	Опрос, реферат

13	Основы технологии виртуальных защищенных сетей VPN.	4			№№ 1-6	Опрос, реферат
14	Мероприятия по выявлению каналов утечки информации	6			№№ 1-6	Опрос, реферат
15	Технологии обнаружения вторжений в компьютерных сетях.	4			№№ 1-6	Опрос, реферат
16	Методы идентификации и аутентификации пользователей компьютерных систем.	6			№№ 1-6	Опрос, реферат
17	Адаптивное управление безопасностью в компьютерных сетях.	4			№№ 1-6	Опрос, реферат
ИТОГО		**76**				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности подготовки реализация компетентностного подхода предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий.

Аудиторная работа включает: лекции, практические занятия, мастер-классы, консультации.

В курсе лекций использованы наглядные, иллюстрированные материалы, обширная информация в табличной и графической формах, а также электронные ресурсы сети Интернет. Разработаны продвинутые лекции (с визуализацией) в формате презентаций, с использованием пакета прикладных программ MS Power Point.

Внеаудиторная работа призвана для формирования и развития профессиональных навыков обучающихся. Самостоятельная работа включает: выполнение домашних заданий, подготовка рефератов, участие в дискуссиях, работа в информационно-образовательной среде. В конце обучения проводится экзамен.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Оценочные средства приведены в ФОС (Приложение А)

7. Учебно-методическое и информационное обеспечение дисциплины Методы оценки безопасности компьютерных систем

Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой _____ **Алиева Ж.А.**

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотеке	На кафедре
Основная				
1.	лк, пз, срс	Вагина, Н. Д. Диагностика и прогнозирование угроз организации : учебно-методическое пособие / Н. Д. Вагина. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2018. — 102 с. — ISBN 978-5-00137-036-9. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/115101	
2.	лк, пз, срс	Кондрашова, Е. А. Финансовая безопасность предприятия : учебно-методическое пособие / Е. А. Кондрашова. — Донецк : ДонНУ, 2020. — 190 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/179971	
3.	лк, пз, срс	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/156401	
Дополнительная				
4.	лк, пз, срс	Международное сотрудничество в области охраны окружающей среды : учебное пособие / Ю. А. Мандра, Е. Е. Степаненко, Т. Г. Зеленская, О. А. Поспелова. — Ставрополь : СтГАУ, 2015. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/82242	
5.	лк, пз, срс	Шилер, А. В. Обеспечение информационной безопасности корпоративных информационных сетей на базе программного комплекса SecureTower : учебно-методическое пособие / А. В. Шилер, А. А. Елизаров, Е. А. Степанова. — Омск : ОмГУПС, 2020. — 23 с. — Текст : электронный // Лань : электронно-	URL: https://e.lanbook.com/book/165730	

		библиотечная система.	
6.	лк, пз, срс	Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; под редакцией В. Н. Ясенева. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2017. — 198 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/153011

8.Материально-техническое обеспечение дисциплины (модуля) «Методы оценки безопасности компьютерных систем»

Материально-техническое обеспечение дисциплины включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.rar (Windows, x86).

8.4. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

При проведения лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС http://library.mirea.ru/.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в

здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене