Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Комплексное обеспечение информационной безопасности автоматизированных систем
наименование дисциплины по ОПОП

для направления 10.03.01 Информационная безопасность
код и полное наименование специальности

по профилю Безопасность автоматизированных систем

факультет Компьютерных технологий энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная , очно-заочная курс 4 семестр (ы) 8(9)
очная, очно-заочная, заочная

г. Махачкала 2024

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению 10.03.01 Информационная безопасность и профилю Безопасность автоматизированных [redacted]

[redacted]

кафедры информационной [redacted] программа одобрена на заседании выпускающей ка безопасности от 15 октября 2024 года, протокол № 3.

[redacted]

«15» октября 2024 г.

Программа одобрена на заседании Методического Совета факультета компьютерных технологий и энергетики от 17 октября 2024 года, протокол № 2 .

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

Декан факультета _____ подпись Т.А. Рагимова ФИО

Начальник УО _____ подпись М.Т. Муталибов ФИО

Проректор по УР _____ подпись А.Ф. Демирова ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Комплексное обеспечение информационной безопасности автоматизированных систем» является изучение основ технологии открытых информационных систем, а именно, взаимодействие открытых информационных систем и переносимости программных продуктов.

Задачи дисциплины: предотвращении и расследовании компьютерных преступлений; предотвращение угроз информационной безопасности объекта; организация службы безопасности объекта; подбор и работа с кадрами в сфере информационной безопасности; организация и обеспечение режима секретности; • охрана объектов.

2.Место дисциплины в структуре ОПОП

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к части, формируемой участниками образовательных отношений).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Технология построения защищенных АС, Безопасность вычислительных сетей, Аудит защищенности информации в автоматизированных системах.

Последующими дисциплинами являются: Преддипломная практика, Подготовка к процедуре защиты и защита выпускной квалификационной работы.

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

В результате освоения дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» студент должен овладеть следующей компетенцией:

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ПК-1	Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ПК-1.1Знает основные методы управления защитой информации. Знает основные угрозы безопасности информации и модели нарушителя автоматизированных системах. Умеет классифицировать и оценивать угрозы безопасности информации в автоматизированных системах. ПК-1.2. Владеет навыками обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы.
ПК-2	Способен осуществлять администрироование средств защиты информации в компьютерных системах и сетях	ПК-2-1. Знает принципы обслуживания и администрирования программно-аппаратных подсистем защиты информации в компьютерных сетях; ПК-2-2. Умеет формулировать и администрировать политики безопасности за счет использования программно-аппаратных средств в компьютерных сетях; ПК-2-3. Имеет практический опыт формирования состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях
ПК-3	Способен осуществлять администрирование подсистем защиты информации в операционных системах	ПК-3-1. Знает принципы обслуживания и администрирования подсистем защиты информации прикладного и системного программного обеспечения ПК-3-2. Умеет формулировать и администрировать политики безопасности прикладного и системного программного обеспечения ПК-3-3. Имеет практический опыт формирования состава применяемых программно-аппаратных средств для обеспечения защиты прикладного и системного программного обеспечения
ПК-4	Способен осуществлять аудит защищенности информации в автоматизированных системах	ПК-4-1. Знает способы проведения анализа безопасности компьютерных систем, способы выявления основных задач и требований при проектировании подсистем защиты ин-формации в компьютерных системах и сетях; ПК-4-2. Умеет проводить анализ проблем безопасности для проектирования подсистем защиты информации в компьютерных системах и сетях; ПК-4-3. Имеет практический опыт применения методов анализа проблем безопасности для проектирования подсистем информационной безопасности распределенных информационных систем

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	3/108	3/108	
Семестр	8	8	
Лекции, час	24	9	
Практические занятия, час	-		
Лабораторные занятия, час	24	9	
Самостоятельная работа, час	24	54	
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)	**1 ЗЕТ – 36 часов**	**1 ЗЕТ – 36 часов**	

4.1.Содержание дисциплины (модуля) «Комплексное обеспечение информационной безопасности автоматизированных 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: Введение. Структура курса. Основные понятия.	2	-	2	4	1		1	6				
2.	Лекция №2: Выбор концептуальной модели построения защиты. Методология формирования задач защиты.	2		2	4	1		1	6				
3.	Лекция №3: Этапы проектирования КСИБ и требования к ним. Структура комплексной системы защиты информации от несанкционированного доступа.	2	-	2	4	1		1	6				
4.	Лекция №4: Мониторинг и контроль состояния окружающей среды. Методы и методики проектирования КСИБ от НСД.	2		2	6	1		1	6				
5.	Лекция №5: Целевая функция задач защиты информации. Особенности построения КСИБ в системах с сосредоточенной обработкой данных. Особенности построения КСИБ в системах с распределенной обработкой данных.	2		2	4	1		1	6				
6.	Лекция №6: Построение системы безопасности информации рабочей станции. Построение КСИБ в глобальных АСУ	2		2	6	1		1	6				
7.	Лекция №7: Методы и методики оценки качества КСИБ.	2		2	4	1		1	6				
8.	Лекция №8: Требования к эксплуатационной документации КСИБ.	2	-	2	4	1		1	6				
9.	Лекция №9: Аттестация по требованиям безопасности. Организационно-функциональные задачи службы безопасности.	1		1	4	1		1	6				

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)	Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого	16	-	16	40	9	-	9	54				

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	№1-4	Анализ и оценка угроз безопасности информации	2	1		№№ 1-5
2	№5-10	Определение потенциальных каналов, методов и возможностей НСД к информации	2	1		№№ 1-5
3	№11-14	Классификация мер обеспечения безопасности компьютерных систем	2	1		№№ 1-5
4	№15-18	Определение компонентов КСЗИ	2	1		№№ 1-5
5	№19-22	Определение условий функционирования КСЗИ	2	1		№№ 1-5
6	№23-26	Разработка модели КСЗИ	2	1		№№ 1-5
7		Назначение, структура и содержание управления КСЗИ	2	1		№№ 1-5
8	№ 27-30	Принципы и методы планирования функционирования КСЗИ	2	1		№№ 1-5
9	№31-34	Сущность и содержание контроля функционирования КСЗИ	1	1		№№ 1-5
ИТОГО			16	9		

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	4	4	5	6	7
1.	Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.	2	2		№№ 1-5	Опрос, реферат, статья
2.	Показатели эффективности инженерно-технической защиты информации.	2	2		№№ 1-5	Опрос, реферат, статья
3.	Способы оптимизации мер инженерно-технической защиты информации.	2	2		№№ 1-5	Опрос, реферат, статья
4.	Разрешение конфликта в условиях рефлексивных игр.	2	2		№№ 1-5	Опрос, реферат, статья
5.	Разработка матрицы конфликтного взаимодействия для типовых ТКС.	2	2		№№ 1-5	Опрос, реферат, статья
6.	Особенности инструментального контроля эффективности инженерно-технической защиты информации.	2	2		№№ 1-5	Опрос, реферат, статья
7.	Оценка дальности перехвата сигналов.	2	4		№№ 1-5	Опрос, реферат, статья
8.	Методический подход к оценке эффективности защиты информации от технических разведок.	2	4		№№ 1-5	Опрос, реферат, статья
9.	Математическая модель канала акустической утечки информации.	2	4		№№ 1-5	Опрос, реферат, статья
10.	Показатели эффективности функционирования средств защиты информации в ТКС.	2	4		№№ 1-5	Опрос, реферат, статья
11.	Скрытие и Комплексное обеспечение ИБ автоматизированных систем.	2	2		№№ 1-5	Опрос, реферат, статья
12.	Фильтрация информационных сигналов.	4	4		№№ 1-5	Опрос, реферат, статья
13.	Скрытие речевой информации в телефонных системах с использованием	2	4		№№ 1-5	Опрос, реферат, статья

	криптографических методов.					
14.	Методы и средства инженерной защиты и технической охраны объектов.	4	4		№№ 1-5	Опрос, реферат, статья
15.	Система охранно-тревожной сигнализации.	2	4		№№ 1-5	Опрос, реферат, статья
16.	Технический контроль эффективности мер защиты информации	4	4		№№ 1-5	Опрос, реферат, статья
17.	Методы испытаний Порядок проведения контроля защищенности АС от НСД.	2	4		№№ 1-5	Опрос, реферат, статья
ИТОГО		40	54			

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению 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

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	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/180100	
2.	лк, пз, срс	Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 с. — ISBN 978-5-9515-0426-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/101929.html	
3.	лк, пз, срс	Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система	URL: https://e.lanbook.com/book/101600 -	
Дополнительная				
4.	лк, пз, срс	Бурова, М. А. Информационная безопасность и защита информации : учебное пособие / М. А. Бурова, А. С. Овсянников. — Самара : СамГУПС, [б. г.]. — Часть 2 — 2012. — 150 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/130272 -	

5.	лк, пз, срс	Голиков, А. М. Комплексное обеспечение ИБ автоматизированных систем : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/110328 -

7. Материально-техническое обеспечение дисциплины (модуля) «Комплексное обеспечение информационной безопасности автоматизированных 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