Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Организационное и правовое обеспечение информационной безопасности
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 3 семестр (ы) 6(7)
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 систем.

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

«27» сентября 2024г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)

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

«15» сентября 2024 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности от 15 октября2024 года, протокол № 3.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)

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

«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 _____ Т.И. Исабекова, к.ф.-м.н., доцент
подпись (ФИО уч. степень, уч. звание)

Декан факультета _____ Т.А. Рагимова
подпись ФИО

Начальник УО _____ М.Т. Муталибов
подпись ФИО

Проректор по УР _____ А.Ф. Демирова
подпись ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности» является дать основы правового обеспечения информационной безопасности, а также формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

Задачи дисциплины: дать основы:

- законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;
- понятий и видов защищаемой информации по законодательству РФ;
- правовых режимов конфиденциальной информации;
- правового режим защиты государственной тайны, системы защиты государственной тайны;
- лицензирования и сертификации в области защиты информации, в том числе государственной тайны;
- правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);
- защиты интеллектуальной собственности;
- правовой регламентации охранной деятельности;
- правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований.
- угроз информационной безопасности объекта;
- организации службы безопасности объекта;
- подбора и работы с кадрами в сфере информационной безопасности;
- организации и обеспечения режима конфиденциальности;
- охраны объектов.

2.Место дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к блоку 1 (обязательная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности, Гуманитарные аспекты информационной безопасности, Правоведение, Гражданское и социально - ответственное поведение, История.

Последующими дисциплинами являются: Комплексное обеспечение ИБ автоматизированных систем.

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

В результате освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» студент должен овладеть следующими компетенциями: УК-10; ОПК-5; ОПК-6; ОПК-8

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)

УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1.1- знает содержание основных нормативных правовых актов в сфере противодействия коррупции УК-10.2.2 - умеет соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1.1 -знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации ОПК-5.1.2 - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-5.1.3 - знает правовые основы организации защиты государственной тайны и конфиденциальной информации ОПК-5.1.4 - знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации ОПК-5.2.1 - умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.1.4 - знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1.2 - знает систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации ОПК-6.1.3 - знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях

ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1.1- знает статус и порядок работы основных правовых информационно-справочных систем

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144	4/144	
Семестр	6	7	
Лекции, час	34	17	
Практические занятия, час	-	-	
Лабораторные занятия, час	34	17	
Самостоятельная работа, час	40	74	
Курсовой проект (работа), РГР, семестр	6	7	
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	1 зет -36	

4.1.Содержание дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности»

№ 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: «Организационные основы и принципы деятельности службы защиты информации».	2	2	-	2	1	1		4				
2	Лекция №2. Тема: «Законодательство РФ в области информационной безопасности».	2	2	-	2	1	1		4				
3	Лекция №3. Тема: «Правовые основы защиты конфиденциальной информации».	2	2	-	2	1	1		4				
4	Лекция №4. Тема: «Правовые основы защиты государственной тайны».	2	2	-	2	1	1		4				
5	Лекция №5. Тема: «Лицензирование и сертификация».	2	2	-	2	1	1		4				
6	Лекция №6. Тема: «Нормы ответственности за правонарушения в сфере компьютерных технологий!.	2	2	-	2	1	1		4				
7	Лекция №7. Тема: «Анализ объекта защиты с позиции организационного обеспечения информационной безопасности».	2	2	-	2	1	1		4				
8	Лекция № 8. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности».	2	2	-	2	1	1		4				
9	Лекция №9. Тема: «Структура службы защиты информации.	2	2	-	2	1	1		4				
10	Лекция №10. Тема: «Организационные основы и принципы деятельности службы защиты информации».	2	2	-	2	1	1		4				
11	Лекция №11. Тема: «Сущность, организация и принципы управления службой защиты информации на предприятии».	2	2	-	2	1	1		4				
12	Лекция №12. Тема: «Методы и технологии управления службой защиты информации на предприятии».	2	2	-	2	1	1		5				
13	Лекция №13. Тема: «Средства и методы физической защиты объектов».	2	2	-	2	1	1		5				
14	Лекция №14. Тема: «Организация службы безопасности и работа с кадрами».	2	2	-	2	1	1		5				

15	Лекция №15. Тема: «Организация и обеспечения режима секретности».	2	2	-	4	1	1		5				
16	Лекция №16. «Организация труда сотрудников подразделения мониторинга информационной безопасности».	2	2	-	4	1	1		5				
17	Лекция №17. Тема: «Организация пропускного и внутри объектового режима».	2	2	-	4	1	1		5				
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				экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		34	34	-	40	17	17		74				

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 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	Организационные основы и принципы деятельности службы защиты информации.	2			№№ 1-7
2	№2	Законодательство РФ в области информационной безопасности.	2			№№ 1-7
3	№3	Правовые основы защиты конфиденциальной информации.	2			№№ 1-7
4	№4	Правовые основы защиты государственной тайны.	2			№№ 1-7
5	№5	Лицензирование и сертификация.	2			№№ 1-7
6	№ 6	Нормы ответственности за правонарушения в сфере компьютерных технологий.	2			№№ 1-7
7	№7	Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	2			№№ 1-7
8	№8	Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.	2			№№ 1-7
9	№9	Структура службы защиты информации.	2			№№ 1-7
10	№10	Организационные основы и принципы деятельности службы защиты информации».	2			№№ 1-7
11	№11	Сущность, организация и принципы управления службой защиты информации на предприятии.	2			№№ 1-7
12	№12	Методы и технологии управления службой защиты информации на предприятии.	2			№№ 1-7
13	№13	Средства и методы физической защиты объектов.	2			№№ 1-7

14	№14	Организация службы безопасности и работа с кадрами.	2			№№ 1-7
15	№15	Организация и обеспечения режима секретности.	2			№№ 1-7
16	№16	Организация труда сотрудников подразделения мониторинга информационной безопасности.	2			№№ 1-7
17	№17	Организация пропускного и внутри объектового режима.	2			№№ 1-7
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	Организационные основы и принципы деятельности службы защиты информации.	2			№№ 1-7	Опрос, реферат, статья
2	Законодательство РФ в области информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья
3	Правовые основы защиты конфиденциальной информации.	2			№№ 1-7	Опрос, реферат, статья
4	Правовые основы защиты государственной тайны.	2			№№ 1-7	Опрос, реферат, статья
5	Лицензирование и сертификация.	2			№№ 1-7	Опрос, реферат, статья
6	Нормы ответственности за правонарушения в сфере компьютерных технологий.	2			№№ 1-7	Опрос, реферат, статья
7	Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья
8	Деятельность по обеспечению	2			№№ 1-7	Опрос, реферат, статья

	информационной безопасности, средства и субъекты обеспечения информационной безопасности.					
9	Структура службы защиты информации.	2			№№ 1-7	Опрос, реферат, статья
10	Организационные основы и принципы деятельности службы защиты информации».	2			№№ 1-7	Опрос, реферат, статья
11	Сущность, организация и принципы управления службой защиты информации на предприятии.	2			№№ 1-7	Опрос, реферат, статья
12	Методы и технологии управления службой защиты информации на предприятии.	2			№№ 1-7	Опрос, реферат, статья
13	Средства и методы физической защиты объектов.	2			№№ 1-7	Опрос, реферат, статья
14	Организация службы безопасности и работа с кадрами.	2			№№ 1-7	Опрос, реферат, статья
15	Организация и обеспечения режима секретности.	4			№№ 1-7	Опрос, реферат, статья
16	Организация труда сотрудников подразделения мониторинга информационной безопасности.	4			№№ 1-7	Опрос, реферат, статья
17	Организация пропускного и внутри объектового режима.	4			№№ 1-7	Опрос, реферат, статья
ИТОГО		40				

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 _____ Сулейманова О.Ш.

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.		Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. — Пенза : ПГУ, 2018. — 186 с. — ISBN 978-5-907102-51-4. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/162235	
2.		Овчинников, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Овчинников. — Санкт-Петербург : ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/216491	
3.	лк, пз, срс	Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/176563	-
Дополнительная				
4.	лк, пз, срс	Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/118230	-
5.	лк, пз, срс	Исследование методов кодирования и шифрования : учебное пособие / А. П. Алексеев, М. И. Макаров, О. В. Сирант,	URL: https://e.lanbook.co	-

		С. С. Яковлева ; под редакцией А. П. Алексеева. — Самара : ПГУТИ, 2018. — 102 с. — Текст : электронный // Лань : электронно-библиотечная система. —	m/book/182252	
6.	лк, пз, срс	Криптографические методы защиты информации : учебное пособие / составители И. А. Калмыков [и др.]. — Ставрополь : СКФУ, 2015. — 109 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/155280	-
7.	лк, пз, срс	Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 91 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/163861	-
8.	лк, пз, срс	Стеганографические и криптографические методы защиты информации : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/90963	-

7. Материально-техническое обеспечение дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности»

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.

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

9. Лист изменений и дополнений к рабочей программе

Дополнения и изменения в рабочей программе на 20___/20___ учебный год.

В рабочую программу вносятся следующие изменения:
1. ……..;
2. ……..;
3. ……..;
4. ……..;
5. ……..
или делается отметка о нецелесообразности внесения каких-либо изменений или дополнений на данный учебный год.

Рабочая программа пересмотрена и одобрена на заседании кафедры _____ от _____ года, протокол № _____.

Заведующий кафедрой _____ _____ _____
(название кафедры) (подпись, дата) (ФИО, уч. степень, уч. звание)

Согласовано:

Декан (директор)_____ _____ _____
(подпись, дата) (ФИО, уч. степень, уч. звание)

Председатель МС факультета _____ _____ _____
(подпись, дата) (ФИО, уч. степень, уч. звание)

Приложение А

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Уровень образования **бакалавриат**
(бакалавриат/магистратура/специалитет)

Направление **10.03.02 Информационная безопасность**
(код, наименование специальности)

Профиль **Безопасность автоматизированных систем**
(наименование)

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

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол № 2

Зав. кафедрой _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Организационное и правовое обеспечение информационной безопасности» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению 10.03.01 Информационная безопасность .

Рабочей программой дисциплины «Организационное и правовое обеспечение информационной безопасности» предусмотрено формирование следующих компетенций:

УК-10 Способен формировать нетерпимое отношение к коррупционному поведению;

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)

- *Курсовая работа / курсовой проект*
- *Устный опрос*
- *Вопросы для проведения экзамена*

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем[1]
УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1.1- знает содержание основных нормативных правовых актов в сфере противодействия коррупции	знать; сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями уметь анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению владеть навыками работы с законодательными и другими нормативными правовыми актами	№№1-17
	УК-10.2.2 - умеет соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей	знать: последствия коррупционной деятельности, в том числе собственных действий или бездействий уметь: анализировать последствия коррупционной деятельности, в том числе собственных действий или бездействий владеть: навыками анализа последствия коррупционной деятельности, в том числе собственных действий или бездействий	№№1-17
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере	ОПК-5.1.1 -знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации	знать: - международные и отечественные нормы и стандарты в области информационных систем и технологий; управление качеством в проектах; - основы конфигурационного управления; предметная область; основы юридических взаимоотношений между контрагентами; инструменты и методы выдачи и контроля поручений. уметь: - перечислить и дать общую характеристику основных нормативно правовых документов в области	№№1-17

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

профессиональной деятельности		ИС; - давать оценку возможностей использования правовых методов защиты в области ИС и технологий; - работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами исправление несоответствий); разрабатывать договоры на основе типовой формы; анализировать входные данные; контролировать выданные поручения. владеть:- навыками эффективного использования поисковых сервисов для отыскания нормативно-Законодательных (законодательные акты, законы РФ и т.д.) в области ИС.	
	ОПК-5.1.2 - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	№№1-17
	ОПК-5.1.3 - знает правовые основы организации защиты государственной тайны и конфиденциальной информации	знает правовые основы организации защиты государственной тайны и конфиденциальной информации	№№1-17
	ОПК-5.1.4 - знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	№№1-17
	ОПК-5.2.1 - умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	№№1-17
ОПК-6 - Способен при	ОПК-5.1.4 - знает правовую	знать:- стандарты РФ в области информационной	№№1-17

решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	безопасности и оборота конфиденциальных документов уметь:- выбрать структуру построения комплексной охраны объекта; правильно выбрать приборы технических средств охраны для заданной схемы построения защиты объекта владеть:- навыками построения системы защищенного документооборота на основе проведенного анализа информационной безопасности объекта информатизации	
	ОПК-6.1.2 - знает систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации	знать:- нормативную и методическую документацию Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. уметь:- оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;.	№№1-17
	ОПК-6.1.3 - знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях	знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях	№№1-17
ОПК-8 - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1.1- знает статус и порядок работы основных правовых информационно-справочных систем	знать:- методы подбора и поиска информации с применением новейших информационных технологий уметь:- пользоваться нормативными документами по защите информации, анализировать и оценивать угрозы информационной безопасности объекта информатизации владеть:- методами анализа применимости тех или иных методов и средств технической разведки для получения информации с конкретного объекта	№№1-17

2.1.1. Этапы формирования компетенций

Сформированность компетенций по дисциплине Организационное и правовое обеспечение информационной безопасности определяется на следующих этапах:

1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2*)

2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
УК-10 Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1.1- знает содержание основных нормативных правовых актов в сфере противодействия коррупции УК-10.2.2 - умеет соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие	ОПК-5.1.1 -знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

деятельность по защите информации в сфере профессиональной деятельности	информации ОПК-5.1.2 - знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-5.1.3 - знает правовые основы организации защиты государственной тайны и конфиденциальной информации ОПК-5.1.4 - знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации ОПК-5.2.1 - умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.1.4 - знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации						
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1.2 - знает систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации ОПК-6.1.3 - знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1.1- знает статус и порядок работы основных правовых информационно-справочных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины Организационное и правовое обеспечение информационной безопасности является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные.

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			**Критерии оценивания**
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

3.1. Задания и вопросы для входного контроля

1. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

Курсовая работа/курсовой проект
Примерные темы курсовых работ/курсовых проектов

Примерные темы курсовых работ/курсовых проектов приводятся в том случае, если данное оценочное средство предусмотрено программой дисциплины.

1. Государственное устройство, силы и средства обеспечения национальной и информационной безопасности в капиталистических странах.
2. Конституция, права и обязанности граждан, теория и практика.
3. Методы и средства защиты государственной тайны в развитых капиталистических странах.
4. Организация режима коммерческой тайны на предприятии.
5. Мировой опыт борьбы с промышленным шпионажем.
6. Безопасность электронной коммерции.
7. Методы и средства защиты интеллектуальной собственности.
8. Мировые политические процессы и внешние угрозы.
9. Преступления в информационной сфере, компьютерные преступления и борьба с ними.
10. Социальная инженерия, методы, возможности, противодействие.
11. Мошенничество в информационной сфере
12. Угрозы физическим лицам при проведении расчетов по банковским картам, безопасность он-лайн платежей.
13. Технология «блокчейн» - содержание, анализ современного состояния, перспективы развития.
14. Мировые цифровые валюты – суть вопроса, правовой статус, анализ современного состояния, перспективы развития.
15. Цифровые следы при работе с электронными устройствами.
16. Методы сокрытия персональной информации в цифровой сфере.
17. Угрозы в сети Интернет, основные правила безопасной работы.

Требования к структуре, содержанию и оформлению курсовых работ (проектов) приводятся в методических указаниях/рекомендациях.

Критерии оценки уровня сформированности компетенций при выполнении курсовой работы/курсового проекта:

- оценка «отлично»: продемонстрировано блестящее владение проблемой исследования, материал выстроен логично, последовательно, обучающийся аргументированно отстаивает свою точку зрения. Во введении приводится обоснование выбора конкретной темы, чётко определены цель и задачи работы (проекта). Использован достаточный перечень источников и литературы для методологической базы исследования. Обучающийся грамотно использует профессиональные термины, актуальные исходные данные. Проведен самостоятельный анализ (исследование) объекта. По результатам работы сделаны логичные выводы. Оформление работы соответствует методическим рекомендациям. Объем и содержание работы соответствует требованиям. На защите обучающийся исчерпывающе отвечает на все дополнительные вопросы;

- оценка «хорошо»: обучающийся демонстрирует повышенный уровень владения проблемой исследования, логично, последовательно и аргументированно отстаивает ее концептуальное содержание. Во введении содержатся небольшие неточности в формулировках цели, задач. В основной части допущены незначительные погрешности в расчетах (в исследовании). Выводы обоснованы, аргументированы. Оформление работы соответствует методическим рекомендациям. Объем работы соответствует требованиям. На защите обучающийся отвечает на все дополнительные вопросы;

- оценка «удовлетворительно»: обучающийся демонстрирует базовый уровень владения проблемой исследования. Во введении указаны цель и задачи исследования, но отсутствуют их четкие формулировки. Работа является компиляцией чужих исследований с попыткой формулировки собственных выводов в конце работы. Изложине материала логично и аргументировано. Наблюдается отступление от требований в оформлении и объеме работы. При ответе на вопросы обучающийся испытывает затруднения;

- оценка «неудовлетворительно»: обнаруживается несамостоятельность выполнения курсовой работы, некомпетентность в исследуемой проблеме. Нарушена логика изложения. Работа не соответствует требованиям, предъявляемым к оформлению и содержанию. На защите курсовой работы обучающийся не отвечает на вопросы.

3.2. Задания для промежуточной аттестации и экзамена

3.2.1 Аттестационная контрольная работа №1

1. Организационные основы и принципы деятельности службы защиты информации.
2. Законодательство РФ в области информационной безопасности.
3. Правовые основы защиты конфиденциальной информации.
4. Правовые основы защиты государственной тайны.
5. Лицензирование и сертификация.

3.2.2 Аттестационная контрольная работа №2

1. Нормы ответственности за правонарушения в сфере компьютерных технологий.
2. Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
3. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
4. Структура службы защиты информации.
5. Организационные основы и принципы деятельности службы защиты информации.

3.2.3 Аттестационная контрольная работа №3

1. Сущность, организация и принципы управления службой защиты информации на предприятии.
2. Методы и технологии управления службой защиты информации на предприятии.
3. Средства и методы физической защиты объектов.
4. Организация службы безопасности и работа с кадрами.
5. Организация и обеспечения режима секретности.

3.3. Список вопросов к зачету и (или) / экзамену

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?

8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Организационные основы и принципы деятельности службы защиты информации.
11. Законодательство РФ в области информационной безопасности.
12. Правовые основы защиты конфиденциальной информации.
13. Правовые основы защиты государственной тайны.
14. Лицензирование и сертификация.
15. Нормы ответственности за правонарушения в сфере компьютерных технологий.
16. Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
17. Деятельность по обеспечению информационной безопасности, средства и субъекты обеспечения информационной безопасности.
18. Структура службы защиты информации.
19. Организационные основы и принципы деятельности службы защиты информации».
20. Сущность, организация и принципы управления службой защиты информации на предприятии.
21. Методы и технологии управления службой защиты информации на предприятии.
22. Средства и методы физической защиты объектов.
23. Организация службы безопасности и работа с кадрами.
24. Организация и обеспечения режима секретности.
25. Организация труда сотрудников подразделения мониторинга информационной безопасности.
26. Организация пропускного и внутри объектового режима.

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

3.4. Вопросы для проверки остаточных знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности»

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.

6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?