Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Основы информационной безопасности
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 1 семестр (ы) 2
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)

«14» 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) «Основы информационной безопасности» является формирование у обучающихся знаний и практических навыков планирования, идентификации и анализа рисков, моделирование рисков, проведение мониторинга.

Задачи дисциплины: ознакомление студентов со: специализированным программным обеспечением, понимание структуры и системы взаимосвязи процессов управления информационной безопасностью; способность и готовность к построению систему управления информационной безопасность предприятия в условиях применения современных информационных технологий.

2.Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к обязательной части учебного плана..

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика.

Последующими дисциплинами являются: Основы управленческой деятельности, Защита программ и данных, Организация работы администратора автоматизированных систем, Защита информации от утечки по техническим каналам, Программно-аппаратные средства защиты информации, Виртуальные частные сети.

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

В результате освоения дисциплины «Основы информационной безопасности» студент должен овладеть следующими компетенциями: ОПК-1.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-1	ОПК-1Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1.1 знает сущность и понятие информации, информационной безопасности и характеристику ее составляющих
		ОПК-1.1.2 знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики
		ОПК-1.1.3 знает источники и классификацию угроз информационной безопасности
		ОПК-1.1.4 знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации
		ОПК-1.1.5 знает основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире
		ОПК-1.2.1 умеет классифицировать и оценивать угрозы информационной безопасности.

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144		
Семестр	2		
Лекции, час	34		
Практические занятия, час	34		
Лабораторные занятия, час	-		
Самостоятельная работа, час	40		
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) «Основы 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: «Понятие информационной безопасности. Основные составляющие»** 1. Определение понятия "информационная безопасность" 2. Доступность, целостность и конфиденциальность информации	2	2	-	2								
2	**Лекция №2** **Тема: «Важность и сложность проблемы информационной безопасности»** 1. Основные понятия угроз ИБ и их классификация 2. Наиболее опасные угрозы ИБ	2	2	-	2								
3	**Лекции №3** **Тема: «Вирусы как угроза информационной безопасности».** 1. Компьютерные вирусы и информационная безопасность. 2. Характерные черты компьютерных вирусов.	2	2	-	2								
4	**Лекция №4** **Тема: «Классификация компьютерных вирусов»** 1. Классификация компьютерных вирусов по среде обитания. 2. Классификация компьютерных вирусов по особенностям алгоритма работы. 3.Классификация компьютерных вирусов по деструктивные возможностям.	2	2	-	2								
5	**Лекция №5** **«Подходы к обеспечению ИБ»** 1 Понятие политики ИБ 2.Принципы формирования политики безопасности	2	2	-	2								

6	**Лекция №6** **Тема: «Комплексный подход формирования ПБ и средства»** 1. Комплексный подход: достоинства и недостатки 2. Средства, используемые в комплексном подходе.	2	2	-	2								
7	**Лекции №7** **Тема: «Законодательный уровень обеспечения информационной безопасности»** 1. Обзор российского законодательства в области информационной безопасности. 2. Обзор зарубежного законодательства в области информационной безопасности.	2	2	-	2								
8	**Лекция №8** **Тема: «Нормативно-правовые основы информационной безопасности в РФ».** 1. Правовые основы информационной безопасности общества. 2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. 3.Ответственность за нарушения в сфере информационной безопасности.	2	2	-	2								
9	**Лекция №9** **Тема: «Стандарты и спецификации в области ИБ»** 1. Основные понятия 2. Механизмы безопасности.	2	2	-	4								
10	**Лекция № 10** **Тема: «Пассивные средства обеспечения ИБ»** 1.Психологические меры 2.Морально-этические меры	2	2	-	2								

11	**Лекция № 11** **Тема: «Характеристика «вирусоподобных» программ. Антивирусные программы»** 1."Intended"-вирусы. 2. Особенности работы антивирусных программ. Классификация антивирусных программ 3. Факторы, определяющие качество антивирусных программ	2	2	-	2								
12	**Лекция № 12** **Тема: «Административный уровень обеспечения информационной безопасности»** 1. Цели, задачи и содержание административного уровня. 2. Разработка политики информационной безопасности.	2	2	-	4								
13	**Лекция № 13** **Тема: «Информационная безопасность вычислительных сетей».** 1. Особенности обеспечения информационной безопасности в компьютерных сетях 2. Сетевые модели передачи данных. 3. Модель взаимодействия открытых систем OSI/ISO. 4. Адресация в глобальных сетях.	2	2	-	4								
14	**Лекция № 14** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Классификация удаленных угроз в вычислительных сетях 2. Типовые удаленные атаки и их характеристика	2	2	-	2								
15	**Лекция № 15** **Тема: «Удаленные угрозы в вычислительных сетях»** 1. Причины успешной реализации удаленных угроз в вычислительных сетях 2. Принципы защиты распределенных вычислительных сетей	2	2	-	2								

16	**Лекция № 16** **Тема: «Механизмы обеспечения информационной безопасности»** 1. Идентификация и аутентификация 2. Криптография и шифрование 3. Методы разграничение доступа.	2	2	-	2								
17	**Лекция № 17** **Тема: «Механизмы обеспечения информационной безопасности»** 1. Регистрация и аудит 2. Межсетевое экранирование 3. Технология виртуальных частных сетей (VPN).	2	2	-	2								
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	-	40								

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	Ответственность за нарушения в сфере информационной безопасности	4			№№ 1-8
2	№2	Стандарты информационной безопасности РФ	4			№№ 1-8

3	№3	Разработка политики информационной безопасности	4			№№ 1-8
4	№ 4	Каналы несанкционированного доступа к информации	4			№№ 1-8
5	№5	Характерные черты компьютерных вирусов	4			№№ 1-8
6	№6	Факторы, определяющие качество антивирусных программ	4			№№ 1-8
7	№7	Адресация в глобальных сетях	4			№№ 1-8
8	№8	Принципы защиты распределенных вычислительных сетей	4			№№ 1-8
9	№9	Технология виртуальных частных сетей (VPN)	2			№№ 1-8
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	Понятие информационной безопасности. Основные составляющие	2			№№ 1-8	Опрос, реферат
2	Важность и сложность проблемы информационной безопасности	2			№№ 1-8	Опрос, реферат
3	Вирусы как угроза информационной безопасности	2			№№ 1-8	Опрос, реферат
4	Классификация компьютерных вирусов	2			№№ 1-8	Опрос, реферат
5	Подходы к обеспечению ИБ	2			№№ 1-8	Опрос, реферат
6	Комплексный подход формирования ПБ и средства	2			№№ 1-8	Опрос, реферат
7	Законодательный уровень обеспечения информационной безопасности	2			№№ 1-8	Опрос, реферат
8	Нормативно-правовые основы информационной безопасности в РФ	2			№№ 1-8	Опрос, реферат
9	Стандарты и спецификации в области ИБ	4			№№ 1-8	Опрос, реферат
10	Пассивные средства обеспечения ИБ	2			№№ 1-8	Опрос,

						реферат
11	Характеристика «вирусоподобных» программ. Антивирусные программы	2			№№ 1-8	Опрос, реферат
12	Административный уровень обеспечения информационной безопасности	4			№№ 1-8	Опрос, реферат
13	Информационная безопасность вычислительных сетей	4			№№ 1-8	Опрос, реферат
14	Удаленные угрозы в вычислительных сетях	4			№№ 1-8	Опрос, реферат
15	Механизмы обеспечения информационной безопасности	4			№№ 1-8	Опрос, реферат
ИТОГО		**40**				

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 30% 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.		Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118233 — Режим доступа: для авториз. пользователей.	
2.		Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный //	Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 — Режим доступа: для авториз. пользователей.	
Дополнительная				
3.	лк, пз, срс	Петренко, В. И. Теоретические основы защиты информации: учебное пособие / В. И. Петренко. — Ставрополь: СКФУ, 2015. — 222 с. — Текст: электронный //	Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247 — Режим доступа: для авториз. пользователей.	
4.	лк, пз, срс	Мызникова, Т. А. Основы информационной безопасности: учебное пособие / Т. А. Мызникова. — Омск: ОмГУПС, 2017. — 82 с. — ISBN 978-5-949-41160-5. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129192 — Режим доступа: для авториз. пользователей.	
5.	лк, пз, срс	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739 — Режим доступа: для авториз. пользователей.	
6.	лк, пз, срс	Секлетова, Н. Н. 1Анализ рынка информационных систем и технологий: учебное	Лань : электронно-библиотечная система.	

		пособие / Н. Н. Секлетова, А. С. Тучкова, О. И. Захарова. — Самара : ПГУТИ, 2018. — 215 с. — Текст : электронный //	— URL: https://e.lanbook.com/book/182310 — Режим доступа: для авториз. пользователей.
7.	лк, пз, срс	Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия: учебное пособие / В. М. Бабушкин. — Казань: КНИТУ-КАИ, 2020. — 256 с. — ISBN 978-5-7579-2463-2. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/193486 — Режим доступа: для авториз. пользователей.
8.	лк, пз, срс	Криулин, А. А. Основы безопасности прикладных информационных технологий и систем: учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва: РТУ МИРЭА, 2020. — 136 с. — Текст: электронный //	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606 — Режим доступа: для авториз. пользователей.

8. Материально-техническое обеспечение дисциплины (модуля) «Основы 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, 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