Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Теоретические основы компьютерной 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 3 семестр (ы) 6
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.
подпись (ФИО уч. степень, уч. звание)

«18» 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) «Теоретические основы компьютерной безопасности» является обучение студентов принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления.

Задачи дисциплины

–получить представление об основных угрозах информационной безопасности и методах противодействия данным угрозам;

–изучить основные формальные математические модели, используемые для анализа защищенности автоматизированных систем;

–изучить методологию проектирования и построения защищенных автоматизированных систем.

2.Место дисциплины в структуре ОПОП

Дисциплина «Теоретические основы компьютерной безопасности» относится к блоку 1 (обязательная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности, Математическая логика и теория алгоритма, Введение в специальность.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Обеспечение ИБ в интеллектуальных системах.

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

В результате освоения дисциплины «Теоретические основы компьютерной безопасности» студент должен овладеть следующими компетенциями:

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	ОПК-3.2.1 - умеет исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач
		ОПК-3.1.20 - знает основные понятия и определения теории информации
ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2.2 - умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144		
Семестр	6		
Лекции, час	34		
Практические занятия, час	-		
Лабораторные занятия, час	17		
Самостоятельная работа, час	93		
Курсовой проект (работа), РГР, семестр	~~6~~		
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)	-		

4.1.Содержание дисциплины (модуля) «Теоретические основы компьютерной 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	Тема: Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации.	2	-	1	4								
2	Тема: Аддитивная модель. Порядковая шкала. Решетка ценности.	2	-	1	4								
3	Тема: Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.	2	-	1	4								
4	Тема: Структура теории компьютерной безопасности. Основные уровни защиты информации.	2	-	1	4								
5	Тема: Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации.	2	-	1	5								
6	Тема: Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак и вредоносных программ	2	-	1	6								
7	Тема: Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа.	2	-	1	6								
8	Тема: Мандатная (полномочная) политика разграничения доступа. Политика безопасности информационных потоков. Политика ролевого разграничения доступа.	2	-	1	6								
9	Тема: Политика изолированной программной среды. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа.	2	-	1	6								
10	Тема: Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расширенная модель Take-Grant. Анализ информационных каналов.	2	-	1	6								

11	Тема: Классическая модель Белла-Лападулы. Свойства безопасности сис-темы в классической модели Белла-ЛаПадула.	2	-	1	6								
12	Тема: Базовая теорема безопасности в классической модели Белла-ЛаПадула. Эквивалентные подходы к определению безопасности модели Белла-Лападулы.	2	-	1	6								
13	Тема: Политика low-watermark в модели Белла-ЛаПадула. Условия и результаты выполнения операций при реализации политики low-watermark в модели Белла-ЛаПадула. Безопасность переходов в классической модели Белла-ЛаПадула.	2	-	1	6								
14	Тема: Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	2	-	1	6								
15	Тема: Общие положения и основные понятия модели систем военных сообщений. Неформальное описание модели систем военных сообщений.	2	-	1	6								
16	Тема: Формальное описание модели систем военных сообщений. Безопасное состояние в модели систем военных сообщений. Безопасность переходов в модели систем военных сообщений.	2	-	1	6								
17	Тема: Определения смыслов безопасности функции переходов в модели систем военных сообщений. Базовая теорема безопасности в модели систем военных сообщений. Теорема о безопасности системы в модели систем военных сообщений.	2	-	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		34	-	17	93								

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	Парольные системы защиты.	4			№№ 1-7
2	№2	Целостность данных. Модель Кларка-Вилсона.	4			№№ 1-7
3	№3	Дискреционная политика разграничения доступа. Матрица безопасности. Модель Харрисона-Руззо-Ульмана.	4			№№ 1-7
4	№4	Модель Take-Grant.	3			№№ 1-7
5	№5	Модель Белла-Лападулы.	2			№№ 1-7
ИТОГО			17			

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		Очно	Очно-заочно	Заочно		
1	2	3	4	5	6	7
1.	Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации.	4			№№ 1-7	Опрос, реферат, статья
2.	Аддитивная модель. Порядковая шкала. Решетка ценности.	4			№№ 1-7	Опрос, реферат, статья
3.	Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.	4			№№ 1-7	Опрос, реферат, статья

4.	Структура теории компьютерной безопасности. Основные уровни защиты информации.	4			№№ 1-7	Опрос, реферат, статья
5.	Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации.	5			№№ 1-7	Опрос, реферат, статья
6.	Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак и вредоносных программ	6			№№ 1-7	Опрос, реферат, статья
7.	Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа.	6			№№ 1-7	Опрос, реферат, статья
8.	Мандатная (полномочная) политика разграничения доступа. Политика безопасности информационных потоков. Политика ролевого разграничения доступа.	6			№№ 1-7	Опрос, реферат, статья
9.	Политика изолированной программной среды. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа.	6			№№ 1-7	Опрос, реферат, статья
10.	Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расширенная модель Take-Grant. Анализ информационных каналов.	6			№№ 1-7	Опрос, реферат, статья
11.	Классическая модель Белла-Лападулы. Свойства безопасности сис-темы в классической модели Белла-ЛаПадула.	6			№№ 1-7	Опрос, реферат, статья
12.	Базовая теорема безопасности в классической модели Белла-ЛаПадула. Эквивалентные подходы к определению безопасности модели Белла-Лападулы.	6			№№ 1-7	Опрос, реферат, статья
13.	Политика low-watermark в модели Белла-ЛаПадула. Условия и результаты выполнения операций при реализации политики low-watermark в модели Белла-ЛаПадула. Безопасность переходов в классической модели Белла-ЛаПадула.	6			№№ 1-7	Опрос, реферат, статья
14.	Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности	6			№№ 1-7	Опрос, реферат, статья

	информации Биба.					
15.	Общие положения и основные понятия модели систем военных сообщений. Неформальное описание модели систем военных сообщений.	6			№№ 1-7	Опрос, реферат, статья
16.	Формальное описание модели систем военных сообщений. Безопасное состояние в модели систем военных сообщений. Безопасность переходов в модели систем военных сообщений.	6			№№ 1-7	Опрос, реферат, статья
17.	Определения смыслов безопасности функции переходов в модели систем военных сообщений. Базовая теорема безопасности в модели систем военных сообщений. Теорема о безопасности системы в модели систем военных сообщений.	6			№№ 1-7	Опрос, реферат, статья
ИТОГО		93				

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
Теоретические основы компьютерной безопасности
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.		Данилов, А. Н. Основы информационной безопасности : учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. — Пермь : ПНИПУ, 2008. — 556 с. — ISBN 978-5-398-00132-7. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/160787	
2.		Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/182491	
3.	лк, пз, срс	Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7970-2. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/169817	-
Дополнительная				
4.	лк, пз, срс	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	-
5.	лк, пз, срс	Фот, Ю. Д. Методы защиты информации : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/159977	-
6.	лк, пз, срс	Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/182305	-
7.	лк, пз, срс	Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/182299	-

5 Материально-техническое обеспечение дисциплины (модуля) «Теоретические основы компьютерной 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/.

Дистрибутив КриптоПро WinLogon и КриптоПро EAP-TLS;

Дистрибутив КриптоПро JCP и КриптоПро JTLS

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)