

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 направления 10.03.01 Информационная безопасность
код и полное наименование направления

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) 5(6)
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 
подпись

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

« 27 » сентября 2024г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)


подпись

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

«15» сентября 2024 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности от 15 октября 2024 года, протокол № 3.

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


подпись

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

«15» октября 2024 г.

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

Председатель Методического совета факультета КТиЭ


подпись

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

Декан факультета


подпись

Т.А. Рагимова
ФИО

Начальник УО


подпись

М.Т. Муталибов
ФИО

Проректор по УР


подпись

А.Ф. Демирова
ФИО

1. Цели и задачи освоения дисциплины.

Цель освоения дисциплины (модуля) «Теоретические основы компьютерной безопасности» состоит в обучении 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).

Последующей дисциплиной являются: Комплексное обеспечение информационной безопасности автоматизированных систем.

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

В результате освоения дисциплины «Теоретические основы компьютерной безопасности» студент должен овладеть следующей компетенцией: ОПК-3

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1.19 - знает основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды)
		ОПК-3.1.20 - знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства)
		ОПК-3.1.21 - знает основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга)
		ОПК-3.2.9 - умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность)

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	2/72	2/72	
Семестр	5	6	
Лекции, час	34	17	
Практические занятия, час	-	-	
Лабораторные занятия, час	34	17	
Самостоятельная работа, час	40	74	
Курсовой проект (работа), РГР, семестр	-	-	
Зачет (при заочной форме 4 часа отводится на контроль)	-	-	
Часы на экзамен (при очной, очно-заочной формах 1 ЗЕТ – 36 часов , при заочной форме 9 часов отводится на контроль)	1 ЗЕТ – 36 часов	1 ЗЕТ – 36 часов	

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

11	Тема: Классическая модель Белла-ЛаПадулы. Свойства безопасности сис-темы в классической модели Белла-ЛаПадула.	2	-	2	2	1		2	5				
12	Тема: Базовая теорема безопасности в классической модели Белла-ЛаПадула. Эквивалентные подходы к определению безопасности модели Белла-ЛаПадулы.	2	-	2	2	1		-	5				
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	-	2	4	1		1	5				
14	Тема: Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	2	-	2	2	1		-	5				
15	Тема: Общие положения и основные понятия модели систем военных сообщений. Неформальное описание модели систем военных сообщений.	2	-	2	4	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	-	2	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	-	2	2	1		1	6				
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 1-5 тема 2 аттестация 6-10 тема 3 аттестация 11-15 тема								Входная конт.работа; Контрольная работа			
Форма промежуточной аттестации (по семестрам)		Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		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 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.	8			№№ 1-7
2.	№2	Целостность данных. Модель Кларка-Вилсона.	8			№№ 1-7
3.	№3	Дискреционная политика разграничения доступа. Матрица безопасности. Модель Харрисона-Руззо-Ульмана.	6			№№ 1-7
4.	№4	Модель Take-Grant.	6			№№ 1-7
5.	№5	Модель Белла-Лападулы.	6			№№ 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
6.	Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации.	2			№№ 1-7	Опрос, реферат, статья
7.	Аддитивная модель. Порядковая шкала. Решетка ценности.	2			№№ 1-7	Опрос, реферат, статья
8.	Анализ угроз информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья

	Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.					
9.	Структура теории компьютерной безопасности. Основные уровни защиты информации.	4			№№ 1-7	Опрос, реферат, статья
10.	Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации.	2			№№ 1-7	Опрос, реферат, статья
11.	Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак и вредоносных программ	2			№№ 1-7	Опрос, реферат, статья
12.	Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа.	2			№№ 1-7	Опрос, реферат, статья
13.	Мандатная (полномочная) политика разграничения доступа. Политика безопасности информационных потоков. Политика ролевого разграничения доступа.	2			№№ 1-7	Опрос, реферат, статья
14.	Политика изолированной программной среды. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа.	2			№№ 1-7	Опрос, реферат, статья
15.	Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расширенная модель Take-Grant. Анализ информационных каналов.	2			№№ 1-7	Опрос, реферат, статья
16.	Классическая модель Белла-Лападулы. Свойства безопасности системы в классической модели Белла-ЛаПадула.	2			№№ 1-7	Опрос, реферат, статья
17.	Базовая теорема безопасности в классической модели Белла-ЛаПадула. Эквивалентные	2			№№ 1-7	Опрос, реферат, статья

	подходы к определению безопасности модели Белла-ЛаПадулы.					
18.	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.	4			№№ 1-7	Опрос, реферат, статья
19.	Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	2			№№ 1-7	Опрос, реферат, статья
20.	Общие положения и основные понятия модели систем военных сообщений. Неформальное описание модели систем военных сообщений.	4			№№ 1-7	Опрос, реферат, статья
21.	Формальное описание модели систем военных сообщений. Безопасное состояние в модели систем военных сообщений. Безопасность переходов в модели систем военных сообщений.	2			№№ 1-7	Опрос, реферат, статья
22.	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			№№ 1-7	Опрос, реферат, статья
ИТОГО		40				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентного 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.				
2.				
3.	лк, пз, срс	Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/97562.html	
Дополнительная				
4.	лк, пз, срс			
5.	лк, пз, срс			
6.	лк, пз, срс	Дацун, Н. Н. Теоретические основы информационных систем : учебно-методическое пособие / Н. Н. Дацун. — Пермь : Пермский государственный национальный исследовательский университет, 2019. — 100 с. — ISBN 978-5-7944-3353-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/123071.html	
7.	лк, пз, срс	Гульятеева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гульятеева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. —	URL: https://www.iprbookshop.ru/91640.html	
8.	лк, пз, срс			

7. 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 проведении 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

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)

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Теоретические основы компьютерной безопасности»

Уровень образования	<u>бакалавриат</u> (бакалавриат/магистратура/специалитет)
Специальность	<u>10.03.01 Информационная безопасность</u> (код, наименование направления)
Специализация	<u>Безопасность автоматизированных систем</u> (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	18
2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)	18
2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП	19
2.1.2. Этапы формирования компетенций	21
2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания	23
2.2.1. Показатели уровней сформированности компетенций на этапах их формирования	23
2.2.2. Описание шкал оценивания	25
3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП	26
3.1. Задания и вопросы для входного контроля	Ошибка! Закладка не определена.
3.2. Оценочные средства и критерии сформированности компетенций .	Ошибка! Закладка не определена.
3.2.1. Эссе по дисциплине «Теоретические основы компьютерной безопасности»	Ошибка! Закладка не определена.
3.2.2. Аттестационная контрольная работа №1	Ошибка! Закладка не определена.
3.2.3. Аттестационная контрольная работа №2	Ошибка! Закладка не определена.
3.2.4. Аттестационная контрольная работа №3	Ошибка! Закладка не определена.
3.2.5. Список вопросов к экзамену	Ошибка! Закладка не определена.

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Теоретические основы компьютерной 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 «Теоретические основы компьютерной безопасности» предусмотрено формирование следующих компетенций:

ОПК-3 - Способен использовать необходимые математические методы для 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)

- *Устный опрос*
- *Курсовая работа / курсовой проект*
- *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
ОПК – 3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1.19 - знает основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды)	Знать: основные понятия и теоремы теории информации и кодирования; Уметь: вычислять количество информации в сообщениях дискретного источника канала связи; Владеть: основными методами кодирования и декодирования информации для различных задач.	№№ 1-
	ОПК-3.1.20 - знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства)	Знать: знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства); основные принципы и способы кодирования и декодирования; Уметь: вычислять количество информации в сообщениях дискретного источника канала связи; Владеть: основными методами кодирования и декодирования информации для различных задач.	
	ОПК-3.1.21 - знает основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования	Знать: основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга); характеристики кодов	

¹ Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

	каналов связи (линейные коды, циклические коды, код Хэмминга)	<p>разного типа, понятие оптимального и помехоустойчивого кодирования;</p> <p>Уметь: кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования; выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач;</p> <p>Владеть: основными методами кодирования и декодирования информации для различных задач.</p>	
	ОПК-3.2.9 - умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность)	<p>Знать: методы исследования кодов и их применений в ЭВМ и системах защиты информации; основные классы кодов, их параметры и алгоритмы кодирования/декодирования;</p> <p>Уметь: вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность);</p> <p>Владеть: основными методами кодирования и декодирования информации для различных задач.</p>	

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Теоретические основы компьютерной 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 промежуточной аттестации	
		Этап текущих аттестаций				18-20 неделя		
		1-5 неделя	6-10 неделя	11-15 неделя	1-17 неделя			
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС			КР/КП
1	2	3	4	5	6	7		
ОПК – 3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1.19 - знает основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды)	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена	
	ОПК-3.1.20 - знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства)	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена	

	ОПК-3.1.21 - знает основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга)	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-3.2.9 - умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность)	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 Теоретические основы компьютерной 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 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	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Базовый (оценка «удовлетворительно», «зачтено»)	<p>Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП.</p> <p>Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения.</p> <p>Обучающимся продемонстрирован базовый уровень освоения компетенции</p>	<p>Обучающийся владеет знаниями основного материала на базовом уровне.</p> <p>Ответы на вопросы оценочных средств неполные, допущены существенные ошибки.</p> <p>Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач</p>
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 пятибалльная, двадцатибалльная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибалльная	двадцатибалльная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> - 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.: <ul style="list-style-type: none"> - 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.: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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. Системы счисления.
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.

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Курсовая работа/курсовой проект

Примерные темы курсовых работ/курсовых проектов

1. Парольные системы защиты.
2. Целостность данных.
3. Модель Кларка-Вилсона.
4. Стеганография.
5. Криптография. Шифрование.
6. Криптография. Электронно-цифровая подпись и хеширование.
7. Субъект-объектная модель. Изолированная программная среда.
8. Работа с матрицей доступов. Домены безопасности.
9. Модель Take-Grant.
10. Нарушение дискреционной политики безопасности программой «Троянский конь».
11. Мандатные политики безопасности.
12. Стандарты в области защиты информации в компьютерных системах.

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, четко 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.

3.2.2. Аттестационная контрольная работа №1

1. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты.
2. Доступ. Информационный поток. Основная аксиома теории защиты информации.
3. Ценность информации. Модели ценности. Решетка ценности и ее свойства.
4. Общая методология построения систем защиты.
5. Принципы построения системы защиты. Каналы утечки информации.
6. Понятие политики безопасности. Субъект-объектная модель политики безопасности.
7. Дискреционная политика безопасности. Определение.
8. Проблема безопасности при атаке вида «Троянский конь».

3.2.3. Аттестационная контрольная работа №1

1. Ролевая и мандатная политика безопасности. Определения.
2. Политика безопасности информационных потоков.
3. Реализация политики безопасности в терминах субъект-объектной модели.
4. Базовая теорема изолированной программной среды (ИПС).
5. Базовая теорема изолированной программной среды (ИПС).
6. Политика изолированной программной среды.

3.2.4. Аттестационная контрольная работа №1

1. Модель Харрисона-Руззо-Ульмана (HRU). Анализ безопасности модели HRU.
2. Теоремы безопасности для модели HRU.
3. Основные положения модели Take-Grant.
4. Анализ механизмов передачи прав доступа для модели Take-Grant.
5. Расширенная модель Take-Grant.
6. Де-факто правила и определение информационных потоков.
7. Замыкание графов доступов и информационных потоков расширенной модели Take-Grant.
8. Анализ путей распространения прав доступа и информационных потоков расширенной модели Take-Grant.
9. Классическая модель Белла-ЛаПадула.
10. Свойства безопасности для классической модели Белла-ЛаПадула.
11. Базовая теорема безопасности для классической модели Белла-ЛаПадула.
12. Политика low-watermark в модели Белла-ЛаПадула.
13. Безопасность переходов для модели Белла-ЛаПадула.
14. Базовая теорема безопасности для модели Белла-ЛаПадула с функцией переходов. Безопасность в смысле администрирования.

3.2.5. Список вопросов к экзамену

15. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты.
16. Доступ. Информационный поток. Основная аксиома теории защиты информации.
17. Ценность информации. Модели ценности. Решетка ценности и ее свойства.

18. Общая методология построения систем защиты.
19. Принципы построения системы защиты. Каналы утечки информации.
20. Понятие политики безопасности. Субъект-объектная модель политики безопасности.
21. Дискреционная политика безопасности. Определение.
22. Проблема безопасности при атаке вида «Троянский конь».
23. Ролевая и мандатная политика безопасности. Определения.
24. Политика безопасности информационных потоков.
25. Реализация политики безопасности в терминах субъект-объектной модели.
26. Базовая теорема изолированной программной среды (ИПС).
27. Базовая теорема изолированной программной среды (ИПС).
28. Политика изолированной программной среды.
29. Модель Харрисона-Руззо-Ульмана (HRU). Анализ безопасности модели HRU.
30. Теоремы безопасности для модели HRU.
31. Основные положения модели Take-Grant.
32. Анализ механизмов передачи прав доступа для модели Take-Grant.
33. Расширенная модель Take-Grant.
34. Де-факто правила и определение информационных потоков.
35. Замыкание графов доступов и информационных потоков расширенной модели Take-Grant.
36. Анализ путей распространения прав доступа и информационных потоков расширенной модели Take-Grant.
37. Классическая модель Белла-ЛаПадула.
38. Свойства безопасности для классической модели Белла-ЛаПадула.
39. Базовая теорема безопасности для классической модели Белла-ЛаПадула.
40. Политика low-watermark в модели Белла-ЛаПадула.
41. Безопасность переходов для модели Белла-ЛаПадула.
42. Базовая теорема безопасности для модели Белла-ЛаПадула с функцией переходов. Безопасность в смысле администрирования.
43. Модель мандатной политики целостности информации Биба.
44. Модель системы военных сообщений (СВС). Неформальное описание модели.
45. Модель системы военных сообщений (СВС). Формальное описание модели.
46. Модель системы военных сообщений (СВС). Безопасность переходов.

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.

Форма экзаменационного билета (пример оформления)

Министерство науки и высшего образования РФ

ФГБОУ ВО "Дагестанский государственный технический университет"

Дисциплина (модуль) Теоретические основы компьютерной безопасности

Код, направление 10.03.0 Информационная безопасность

профиль Безопасность автоматизированных систем

Кафедра ИБ Курс 3 Семестр 5

Форма обучения – очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

1. Политика изолированной программной среды.
2. Анализ механизмов передачи прав доступа для модели Take-Grant.
3. Классическая модель Белла-ЛаПадула. Свойства безопасности для классической модели Белла-ЛаПадула.

Экзаменатор.....Качаева Г.И.

Утвержден на заседании кафедры (протокол №__ от _____ 20__ г.)

Зав. кафедрой (название)Качаева Г.И.

В ФОС размещается пример заполненного экзаменационного билета. Весь комплект экзаменационных билетов по дисциплине хранится на кафедре в соответствии с утвержденной номенклатурой дел.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;

- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка «отлично»: обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл

основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»**: обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»**: обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»**: обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).