Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Защита информации
наименование дисциплины по ОПОП

для направления 09.03.04 Программная инженерия
код и полное наименование направления (специальности)

по профилю Разработка программно-информационных систем

факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационной безопасности

Форма обучения очная, заочная курс 4/5 семестр (ы) 8/9
очная, очно-заочная, заочная

г. Махачкала 2019

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.04 Программная инженерия с учетом рекомендаций и ОПОП ВО по направлению 09.03.04 Программная инженерия и профилю Разработка программно-информационных систем.

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

«18» 06 2019 г.

Зав. кафедрой, за которой закреплена дисциплина (модуль) Защита информации

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

«18» 06 2019 г.

Программа одобрена на заседании выпускающей кафедры **программного обеспечения вычислительной техники и автоматизированных систем**

от «20» июня 2019 года, протокол № 10 .

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

_____ Айгумов Т.Г., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

«20» 06 2019 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от 12.09 2019 года, протокол № 1 .

Председатель Методического совета факультета КТВТиЭ

_____
подпись (ФИО уч. степень, уч. звание)

«12» 09 2019г.

Декан факультета _____ Юсуфов Ш.А.
подпись ФИО

Начальник УО _____ Магомаева Э.В.
подпись ФИО

И.о начальника УМУ _____ Гусейнов М.Р.
подпись ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Защита информации» является формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

Основные задачи, на решение которых нацелен курс:

- сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер;
- изучить базовые теоретические понятия, лежащие в основе процесса защиты информации, сервисы и механизмы безопасности;
- получить представление о компьютерной криптографии, включающей программную реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей, автоматизацию работы по анализу перехвата и раскрытию шифров;
- научиться использованию криптографических алгоритмов шифрования, электронной цифровой подписи, хэш-функций, генерации псевдослучайных последовательностей чисел и протоколов аутентификации, используемых в широко распространенных программных продуктах.

2.Место дисциплины в структуре ОПОП

Дисциплина «Защита информации» относится к части, формируемая участниками образовательных отношений.

Предшествующими дисциплинами, формирующими начальные знания, являются: «Информатика», «Операционные системы».

Последующими являются: «Преддипломная практика», «Подготовка к сдаче и сдача государственного экзамена», «Выполнение и защита выпускной квалификационной работы».

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

В результате освоения дисциплины Защита информации студент должен овладеть следующими компетенциями: УК-1; ПК-2.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
УК - 1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации
		УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности
		УК-1.3. Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов
ПК - 2	Владение методами контроля проекта и готовностью осуществлять контроль версий	ПК-2.1. Знает основные методы информационной безопасности ИС
		ПК-2.2. Умеет организовать работы по управлению проектом ИС
		ПК-2.3. Имеет навыки в проведении переговоров и способен осуществлять контроль версий

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	3/108		3/108
Семестр	8		9
Лекции, час	16		4
Практические занятия, час	-		-
Лабораторные занятия, час	16		4
Самостоятельная работа, час	40		91
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		9 ч на контроль

4.1. Содержание дисциплины (модуля)

№ 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 №1. Основные понятия и определения в области информационной безопасности. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак.	2	-	2	4								10
2	Тема №2. Традиционное шифрование: классические методы. Криптостойкость. Основные понятия и определения. Подстановочные и перестановочные шифры. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.	2	-	2	4							1	10
3	Тема №3. Алгоритмы генерации псевдослучайных последовательностей чисел. Различные способы создания псевдослучайных чисел.	2	-	2	4								11
4	Тема №4. Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.	2	-	2	6					1		1	12
5	Тема №5. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.	2	-	2	6					1		1	12

6	Тема №.6. Блочные и поточные алгоритмы симметричного шифрования. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля.	2	-	2	6					1		1	12
7	Тема №7. Тема: Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Описание алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения.	2	-	2	4					1			12
8	Тема №8. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael. Асимметричные системы шифрования (системы с открытым ключом). RSA.Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.	2	-	2	6								12
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- 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				экзамен			
Итого		16	-	16	40					4		4	91

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	1-2	Шифрование информации методами традиционного шифрования. Генерация псевдослучайных последовательностей чисел в системах защиты информации.	2			№№ 1-6
2	1-4	Хэш-функции и электронная цифровая подпись.	2			№№ 1-6
3	1-5	Изучение американского стандарта шифрования данных DES. Изучение отечественного стандарта шифрования данных (ГОСТ 28147-89).	2		1	№№ 1-6
4	1-6	Симметричный криптографический алгоритм с AES – подобной структурой Rijndael.	4		1	№№ 1-6
5	1-7	Асимметричные криптосистемы. Шифрование и электронная цифровая подпись на основе с помощью алгоритма RSA.	4		1	№№ 1-6
6	1-8	Выработка общего секретного ключа по алгоритму Диффи – Хэллмана.	2		1	№№ 1-6
ИТОГО			**16**		**4**	

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	№№ 1-6	Опрос, реферат, статья
1.	Основные понятия и определения в области информационной безопасности.	2		6	№№ 1-6	Опрос, реферат, статья
2.	Традиционное шифрование: классические методы. Криптостойкость.	4		8	№№ 1-6	Опрос, реферат, статья
3.	Алгоритмы генерации псевдослучайных последовательностей чисел.	4		10	№№ 1-6	Опрос, реферат, статья
4.	Хэш-функции и аутентификация сообщений.	4		10	№№ 1-6	Опрос, реферат, статья
5.	Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП.	4		10	№№ 1-6	Опрос, реферат, статья
6.	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы.	4		8	№№ 1-6	Опрос, реферат, статья
7.	Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.	4		7	№№ 1-6	Опрос, реферат, статья
8.	Асимметричные системы шифрования	4		8	№№ 1-6	Опрос, реферат, статья
9.	Криптография с использованием эллиптических кривых.	4		8	№№ 1-6	Опрос, реферат, статья
10.	Безопасность современных сетевых технологий. Протоколы аутентификации.	4		8	№№ 1-6	Опрос, реферат, статья
11.	Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.	2		8	№№ 1-6	Опрос, реферат, статья
ИТОГО		**40**		**91**		

5. Образовательные технологии

В рамках дисциплины «Защита информации» уделяется особое внимание установлению межпредметных связей, демонстрации возможности применения полученных знаний в практической деятельности.

В лекционных занятиях используются следующие инновационные методы:

- групповая форма обучения — форма обучения, позволяющая обучающимся эффективно взаимодействовать в микрогруппах при формировании и закреплении знаний;
- компетентностный подход к оценке знаний — это подход, акцентирующий внимание на результатах образования, причем в качестве результата рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях;
- личностно-ориентированное обучение — это такое обучение, где во главу угла ставится личность обучаемого, ее самобытность, самоценность, субъективный опыт каждого сначала раскрывается, а затем согласовывается с содержанием образования;
- междисциплинарный подход — подход к обучению, позволяющий научить студентов самостоятельно «добывать» знания из разных областей, группировать их и концентрировать в контексте конкретной решаемой задачи;
- развивающее обучение — ориентация учебного процесса на потенциальные возможности человека и их реализацию. В концепции развивающего обучения учащийся рассматривается не как объект обучающих воздействий учителя, а как самоизменяющийся субъект учения.

В процессе выполнения лабораторных работ используются следующие методы:

- исследовательский метод обучения — метод обучения, обеспечивающий возможность организации поисковой деятельности обучаемых по решению новых для них проблем, в процессе которой осуществляется овладение обучаемыми методами научными познания и развитие творческой деятельности;
- метод рейтинга — определение оценки деятельности личности или события. В последние годы начинает использоваться как метод контроля и оценки в учебно-воспитательном процессе;
- проблемно-ориентированный подход — подход к обучению позволяющий сфокусировать внимание студентов на анализе и разрешении какой-либо конкретной проблемной ситуации, что становится отправной точкой в процессе обучения.

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 Защита информации

Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой _____ **Алиева Ж.А.**

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотеке	На кафедре
Основная				
1.	лк, пз, срс	Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/188703	
2.	лк, пз, срс	Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/102069.html	
3.	лк, пз, срс	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	-
Дополнительная				
4.	лк, пз, срс	Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/89451.html	-
5.	лк, пз,	Солонская, О. И. Средства защиты	URL:	-

	срс	информации : учебное пособие / О. И. Солонская. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. — 89 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	https://www.iprbookshop.ru/117115.html	
6.	лк, пз, срс	Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/130184	-

8. **Материально-техническое обеспечение дисциплины «Защита информации»**

Материально-техническое обеспечение включает в себя:

- для проведения лекционных и практических занятий на кафедре ПОВТиАС имеется комплект технических средств обучения в составе:
  - интерактивная доска Smart Tehnologies Smart Board V280;
  - моноблок ASUS V2201-BUK (2201-BC022M) Celeron N3050/1GGz/4Gb/500Gb/21,5" FHD/int Intel HD/DVD-SM/Wi-Fi+BT Cam/KB+M/DOS Black;
  - проектор ViewSonic PJD6221 DLP2700 Lumens XGA(1024x768) 2800:1 2,7kg, Audio in/out, Brilliant color.
- Для проведения лабораторных занятий имеются два компьютерных класса, оборудованных компьютерами с установленным программным обеспечением.

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 2020/2021 учебный год.

В рабочую программу вносятся следующие изменения:
1. Изменений нет;
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 ПОВТиАС от 12 09 2020 года, протокол № 1.

Заведующий кафедрой ПОВТиАС _____ Нигматов Т.Г.
(подпись, дата) (ФИО, уч. степень, уч. звание)

Согласовано:

Декан _____ Ш.А. Юсуфов
(подпись, дата) (ФИО, уч. степень, уч. звание)

Председатель МС факультете _____ Т.Ш. Исабекова
(подпись, дата) (ФИО, уч. степень, уч. звание)