Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 07.11.2025 09:36:15
Уникальный программный ключ:
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Криптографические протоколы
наименование дисциплины по ОПОП

для направления 10.03.01 Информационная безопасность
код и полное наименование направления (специальности)

по профилю Безопасность автоматизированных систем

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

кафедр Информационной безопасности.
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 2 семестр (ы) 4.
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)

«18» 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль) Технологии и методы программирования _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

«18» 09 2021г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 20 сентября 2021 года, протокол №.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)
_____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«20» 09 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от 18.10 2021 года, протокол № 1.

Председатель Методической комиссии факультета КТВТиЭ
_____
подпись (ФИО уч. степень, уч. звание)

«18» 09 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) Криптографические протоколы являются ознакомление существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Задача дисциплины «Криптографические протоколы» – получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

2.Место дисциплины в структуре ОПОП

Данная дисциплина **относится к блоку 1 (обязательная часть)** направления подготовки «Информационная безопасность». Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Алгебра и геометрия», «Дискретная математика», «Информатика», «Основы теории кодирования».

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

В результате освоения дисциплины Криптографические протоколы *студент должен овладеть следующими компетенциями:ОПК-2, ОПК-9*

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1.3 - знает типовые структуры и принципы организации компьютерных сетей назначение, функции и обобщённую структуру операционных систем назначение и основные компоненты систем баз данных
		ОПК-2.2.1 - умеет применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет
		ОПК-2.2.2 - умеет составлять SQL запросы и осуществлять удалённый доступ к базам данных
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1.2 - знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	5/180		
Семестр	4		
Лекции, час	34		
Практические занятия, час	34		
Лабораторные занятия, час	34		
Самостоятельная работа, час	42		
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=36ч		

4.1. Содержание дисциплины (модуля) Криптографические протоколы

№ 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: Общие сведения о криптографических протоколах.	2	2	2	2								
2.	Тема №2: Основные понятия. Анализ безопасности простейших протоколов. Классификация атак. Анализ протоколов цифровых подписей. Анализ DSA и ГОСТ.	2	2	2	2								
3.	Тема №3: Привязка к биту и электронная жеребьевка. Компьютерная реализация схем электронной жеребьевки и привязки к биту.	2	2	2	2								
4.	Тема №4: Разделение секрета. Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа.	2	2	2	2								
5.	Тема №5: Разделение секрета. Проверяемое разделение секрета и конфиденциальные вычисления.	2	2	2	3								
6.	Тема №6: Идентификация и аутентификация. Парольные схемы. Одноразовые пароли.	2	2	2	2								
7.	Тема №7: Идентификация и аутентификация. Схемы рукопожатия.	2	2	2	2								
8.	Тема №8: Протоколы идентификации с нулевым разглашением. Интерактивные системы доказательства.	2	2	2	3								
9.	Тема №9: Протоколы идентификации с нулевым разглашением Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.	2	2	2	2								

10.	Тема №10: Протоколы открытых сделок. Компьютерная реализация схем слепой подписи и скрытого канала. Компьютерная реализация протокола «Покер по телефону» для 3-х игроков. Имитационное моделирование схемы электронных денег с монетами одинакового достоинства.	2	2	2	3									
11.	Тема №11: Протоколы обмена ключами	2	2	2	2									
12.	Тема №12: Развитые протоколы обмена ключами с аутентификацией сторон.	2	2	2	3									
13.	Тема №13: Инфраструктура открытых ключей. Изучение работы с удостоверяющим центром при помощи CryptoPro. Формирование и проверка сертификата с использованием CryptoPro.	2	2	2	2									
14.	Тема №14: Управление ключами. Компьютерная реализация протокола передачи секретного ключа через доверенный центр (работа в группах). Компьютерная реализация протокола передачи секретного ключа средствами асимметричной криптографии(работа в группах).	2	2	2	3									
15.	Тема №15: Типичные атаки на протоколы аутентификации. Протоколы защиты данных в сети Internet.	2	2	2	3									
16.	Тема №16: Депонирование ключей и возможность контроля информационного взаимодействия.	2	2	2	3									
17.	Тема №17: Прикладные протоколы. Протоколы семейства KriptoKnight для различных сетевых конфигураций и условий применения. Протоколы семейства IPSec. Протоколы семейства SSL/TLS.	2	2	2	3									
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная Конт. Работа 1 аттестация 1-4 тема 2 аттестация 5-7 тема 3 аттестация 8-10 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	42									

тические занятия, лабораторные работы, контрольные работы, коллоквиумы, тирование (курсовая работа). Вуз может устанавливать другие виды учебных

аттестации в соответствии со сроками проведения текущих аттестаций. По нца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче

тических занятий

Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
Очно	Очно-заочно	Заочно	
4	5	6	7
4			№№1-8
4			№№1-8
4			№№1-8
2			№№1-8
4			№№1-8
4			№№1-8
6			№№1-8
6			№№1-8
34			

ендуемая литература одические разработки сточника из списка литературы)
7
№№1-8
№№1-8
№№1-8
№№1-8
№№1-8
№№1-8
№№1-8
№№1-8

ы контроля СРС
7
, реферат, статья
, реферат, статья

ться	ться	ться	ться	ться	ться	ться	ться	ться	ться	ться	ться	ться	ться	ться	

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.	лк, пз, срс	Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/97571.html	
2.	лк, пз, срс	Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/176563	
3.	лк, пз, срс	Корниенко, А. А. Криптографические протоколы : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2020. — 74 с. — ISBN 978-5-7641-1509-2. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/191009	-
4.	лк, пз, срс	Донгак, Ш. М. Криптография: Практикум : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/163935	
5.	лк, пз, срс	Косолапов, Ю. В. Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов. — Ростов-на-Дону, Таганрог : Издательство	URL: https://www.iprbookshop.ru/10	

		Южного федерального университета, 2020. — 98 с. — ISBN 978-5-9275-3316-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	0176.html	
Дополнительная				
6.	лк, пз, срс	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. — Самара : ПГУТИ, 2019. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/223319	-
7.	лк, пз, срс	Пугин, В. В. Криптографические протоколы : методические указания / В. В. Пугин, С. А. Лабада. — Самара : ПГУТИ, 2018. — 51 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/182303	-
8.	лк, пз, срс	Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. П. Просихин, В. А. Яковлев. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2014. — 277 с. — ISBN 978-5-89160-097-3. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/181501	-

7. Материально-техническое обеспечение дисциплины (модуля) «Криптографические протоколы»

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).

КриптоПро OCSPCOM (версия 1.05.0726).

КриптоПро TSPCOM (версия 1.05.0972).

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 переcмотрена 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)