Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 06.11.2025 10:17:19
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		

[redacted]

[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]ная Конт. Работа; [redacted]трольная работа		
[redacted] / зачет с оценкой/ экзамен		
[redacted]		

К видам учебной работы в вузе отнесены: лекции, консультации, семинары, практические занятия, лабораторные работы, контрольные работы, коллоквиумы, самостоятельные работы, научно- исследовательская работа, практики, курсовое проектирование (курсовая работа). Вуз может устанавливать другие виды учебных занятий.

** - Разделы, тематику и вопросы по дисциплине следует разделить на три текущие аттестации в соответствии со сроками проведения текущих аттестаций. По материалу программы, пройденному студентом после завершения 3-ей аттестации до конца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче зачета или экзамена.*

4.2. Содержание практических занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Очно-заочно	Заочно	
1	2	3	4	5	6	7
1.	4	Идентификация и аутентификация	4			№№1-8
2.	4	Протоколы обмена ключами	4			№№1-8
3.	5	Протоколы обмена ключами	4			№№1-8
4.	6	Протоколы обмена ключами	2			№№1-8
5.	7	Развитые протоколы обмена ключами с аутентификацией сторон	4			№№1-8
6.	8	Депонирование ключей и возможность контроля информационного взаимодействия	4			№№1-8
7.	9	Инфраструктура открытых ключей. Схемы обязательств	6			№№1-8
8.	10	Инфраструктура открытых ключей. Схемы обязательств	6			№№1-8
ИТОГО			34			

4.2. Содержание лабораторных 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
9.	4	Идентификация и аутентификация	4			№№1-8
10.	4	Протоколы обмена ключами	4			№№1-8
11.	5	Протоколы обмена ключами	4			№№1-8
12.	6	Протоколы обмена ключами	2			№№1-8
13.	7	Развитые протоколы обмена ключами с аутентификацией сторон	4			№№1-8
14.	8	Депонирование ключей и возможность контроля информационного взаимодействия	4			№№1-8
15.	9	Инфраструктура открытых ключей. Схемы обязательств	6			№№1-8
16.	10	Инфраструктура открытых ключей. Схемы обязательств	6			№№1-8
ИТОГО			34			

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		Очно	Очно-заочно	Заочно		
1	2	3	4	5	6	7
1.	Общие сведения о криптографических протоколах.	2			№№1-8	Опрос, реферат, статья
2.	Основные понятия. Анализ безопасности простейших протоколов.	2			№№1-8	Опрос, реферат, статья

3.	Привязка к биту и электронная жеребьевка.	2			№№1-8	Опрос, реферат, статья
4.	Разделение секрета.	2			№№1-8	Опрос, реферат, статья
5.	Разделение секрета.	3			№№1-8	Опрос, реферат, статья
6.	Идентификация и аутентификация.	2			№№1-8	Опрос, реферат, статья
7.	Идентификация и аутентификация.	2			№№1-8	Опрос, реферат, статья
8.	Протоколы идентификации с нулевым разглашением.	3			№№1-8	Опрос, реферат, статья
9.	Протоколы идентификации с нулевым разглашением.	2			№№1-8	Опрос, реферат, статья
10.	Протоколы открытых сделок.	3			№№1-8	Опрос, реферат, статья
11.	Протоколы обмена ключами	2			№№1-8	Опрос, реферат, статья
12.	Развитые протоколы обмена ключами с аутентификацией сторон.	3			№№1-8	Опрос, реферат, статья
13.	Инфраструктура открытых ключей.	2			№№1-8	Опрос, реферат, статья
14.	Управление ключами.	3			№№1-8	Опрос, реферат, статья
15.	Типичные атаки на протоколы аутентификации.	3			№№1-8	Опрос, реферат, статья
16.	Депонирование ключей и возможность контроля информационного взаимодействия.	3			№№1-8	Опрос, реферат, статья
17.	Прикладные протоколы. сетевых конфигураций и условий применения.	3			№№1-8	Опрос, реферат, статья
ИТОГО		**42**				

5. Образовательные технологии

Чтение лекций и практические занятия по данной дисциплине проводятся традиционным способом. При работе используется диалоговая форма ведения лекций и практики с постановкой и решением проблемных задач, обсуждением дискуссионных моментов и т.д. При проведении контрольных работ студентам предлагается ответить на некоторые теоретические вопросы по курсу лекций и решить задачи, содержащие элементы научных исследований, которые могут потребовать углубленной самостоятельной проработки теоретического материала. При организации внеаудиторной самостоятельной работы по данной дисциплине преподавателю рекомендуется использовать следующие ее формы:

- решение студентом самостоятельных задач обычной сложности, направленных на закрепление знаний и умений;
- выполнение индивидуальных заданий повышенной сложности, направленных на развитие у студентов научного мышления и инициативы.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Оценочные средства приведены в ФОС (Приложение А)

7. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература и источники информации (основная и дополнительная)

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

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотеке	На кафедре
		Основная		
1.	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 индивиду[redacted]

9. Лист изменений и дополнений к рабочей программе

[redacted]

Дополнения и изменения в рабочей программе на 20___/20___ учебный год.

В рабочую программу вносятся следующие изменения:

1. ……;
2. ……;
3. ……;
4. [redacted]