Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Инфраструктура открытых ключей в СЗИ
наименование дисциплины по ОПОП

для специальности 10.05.03 Информационная безопасность автоматизированных систем
код и полное наименование специальности

по специализации Безопасность открытых информационных систем

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

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 4 семестр (ы) 8
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)

«16» 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)_____
_____ Качаева Г.И.,к.э.н.
подпись (ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 20 сентября 2021 года, протокол № 2 .

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

«20» сентября 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от «18» октября 2021 г., протокол № 2

Председатель Методического совета факультета КТВТиЭ
_____ Исабекова Т.И., к.ф-м.н., доцент
подпись (ФИО уч. степень, уч. звание)

от «18» октября 2021 г.

Декан факультета _____ Юсуфов Ш.А.
подпись ФИО

Начальник УО _____ Магомаева Э.В.
подпись ФИО

И.о проректора по УР _____ Баламирзоев Н.Л.
подпись ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Инфраструктура открытых ключей в СЗИ» является формирование у обучающихся знаний и практических навыков по проектированию и управлению инфраструктурой открытых ключей.

Задачи дисциплины: сформировать представление об основных проблемах, связанных с практическим использование криптографических методов защиты информации; криптографические протоколы; изучить инфраструктуру открытого ключа.

2.Место дисциплины в структуре ОПОП

Дисциплина «Инфраструктура открытых ключей в СЗИ» к относится к обязательной части учебного плана.

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Криптографические методы защиты информации, Математическая логика и теория алгоритма, Безопасность систем баз данных.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Организация работы администратора автоматизированных систем.

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

В результате освоения дисциплины «Инфраструктура открытых ключей в СЗИ» студент должен овладеть следующими компетенциями: ОПК-10.

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.1 - знает принципы организации и структуру систем защиты информации современных операционных систем
		ОПК-10.2.1 - умеет конфигурировать параметры системы защиты информации современных операционных систем
		ОПК-10.1.3 - знает основные протоколы, используемые для защиты информации в вычислительных сетях

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144		
Семестр	8		
Лекции, час	34		
Практические занятия, час	34		
Лабораторные занятия, час	-		
Самостоятельная работа, час	76		
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)	-		

4.1.Содержание дисциплины (модуля) «Инфраструктура открытых ключей в СЗИ»

№ 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: Обзор инфраструктуры открытых ключей (PKI) Введение в PKI. Введение в криптографию. Знакомство с российскими криптоалгоритмами. КриптоПро CSP. Сертификаты и удостоверяющие центры.	2	2	-	4								
2	Тема №2: Планирование иерархии удостоверяющих центров. Требования, влияющие на структуру иерархии удостоверяющих центров. Типовые решения иерархии удостоверяющих центров	2	2	-	4								
3	Тема №3 Планирование иерархии удостоверяющих центров Защита службы управления ключами на удостоверяющем управлением Windows Server 2016/2019 при помощи ПАКМ «КриптоПро HSM».	2	2	-	4								
4	Тема №4: Создание иерархии удостоверяющих центров. Создание удостоверяющего центра, отключенного от сети. Проверка запросов на сертификат.	2	2	-	4								
5	Тема №5: Создание иерархии удостоверяющих центров. Планирование публикации списков отозванных сертификатов. Установка подчиненного удостоверяющего центра.	2	2	-	4								
6	Тема №6: Управление инфраструктурой открытых ключей Введение в управление PKI. Управление сертификатами. Списки отозванных сертификатов.	2	2	-	4								
7	Тема №7: Управление инфраструктурой открытых ключей Протокол OCSP. Сетевой ответчик. Особенности применения КриптоПро OCSP. Управление удостоверяющими центрами. Планирование аварийного восстановления.	2	2	-	4								
8	Тема №8: Настройка шаблонов сертификатов. Введение в шаблоны сертификатов. Разработка и создание шаблона сертификатов. Публикация шаблона сертификатов. Управление изменениями в шаблонах сертификатов.	2	2	-	4								

9	Тема №9: Настройка выпуска сертификатов Введение в выпуск сертификатов. Ручной выпуск сертификатов. Автоматический выпуск сертификатов.	2	2	-	4								
10	Тема №10: Настройка архивирования и восстановления ключей Введение в архивирование и восстановление ключей. Внедрение ручного архивирования и восстановления ключей. Внедрение автоматического архивирования и восстановления ключей.	2	2	-	6								
11	Тема №11: Обеспечение конфиденциальности данных Архитектура EFS. Шифрование данных с помощью EFS. Особенности применения КриптоПро EFS.	2	2	-	6								
12	Тема №12: Обеспечение конфиденциальности данных Обеспечение конфиденциальности данных. Архитектура EFS. Шифрование данных с помощью EFS. Особенности применения КриптоПро EFS.	2	2	-	4								
13	Тема №13: Настройка доверия между организациями Дополнительные вопросы, связанные с иерархией удостоверяющих центров. Настройка ограничений в файле Policy.inf. Возможности квалифицированного подчинения.	2	2	-	4								
14	Тема №14: Внедрение смарт-карт Введение в смарт-карты. Выпуск сертификатов для смарт-карт. Внедрение смарт-карт. Применение биометрической идентификации в смарт-картах. Особенности применения КриптоПро WinLogon.	2	2	-	6								
15	Тема №15: Защита трафика с применение криптографии Введение в SSL/TLS. Включение SSL/TLS на web-сервере. Особенности применения КриптоПро TLS.	2	2	-	4								
16	Тема №16: № 6 Защита трафика с применение криптографии Внедрение аутентификации на основе сертификатов. Введение в IPsec. Особенности применения КриптоПро IPsec.	2	2	-	6								
17	Тема №17: Настройка защищенной электронной почты Введение в защищенную электронную почту. Настройка защиты для электронного письма. Восстановление секретного ключа для электронной почты.	2	2	-	4								

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/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен				
Итого	34	34	-	76									

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	Обзор инфраструктуры открытых ключей (PKI)	2			№№ 1-8
2	№2	Планирование иерархии удостоверяющих центров	4			№№ 1-8
3	№3	Создание иерархии удостоверяющих центров	4			№№ 1-8
4	№4	Управление инфраструктурой открытых ключей	2			№№ 1-8
5	№5	Настройка шаблонов сертификатов	4			№№ 1-8
6	№ 6	Настройка выпуска сертификатов	2			№№ 1-8
7	№7	Настройка архивирования и восстановления ключей	2			№№ 1-8
8	№8	Обеспечение конфиденциальности данных	2			№№ 1-8
9	№9	Настройка доверия между организациями	2			№№ 1-8
10	№10	Внедрение смарт-карт	2			№№ 1-8
11	№11	Защита трафика с применение криптографии	4			№№ 1-8
12	№12	Настройка защищенной электронной почты	4			№№ 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.	Обзор инфраструктуры открытых ключей (PKI) Введение в PKI. Введение в криптографию. Знакомство с российскими криптоалгоритмами. КриптоПро CSP. Сертификаты и удостоверяющие центры.	4			№№ 1-8	Опрос, реферат, статья
2.	Планирование иерархии удостоверяющих центров. Требования, влияющие на структуру иерархии удостоверяющих центров. Типовые решения иерархии удостоверяющих центров.	4			№№ 1-8	Опрос, реферат, статья
3.	Планирование иерархии удостоверяющих центров Защита службы управления ключами на удостоверяющем управлением Windows Server 2016/2019 при помощи ПАКМ «КриптоПро HSM».	4			№№ 1-8	Опрос, реферат, статья
4.	Создание иерархии удостоверяющих центров. Создание удостоверяющего центра, отключенного от сети. Проверка запросов на сертификат.	4			№№ 1-8	Опрос, реферат, статья
5.	Создание иерархии удостоверяющих центров. Планирование публикации списков отозванных сертификатов. Установка подчиненного удостоверяющего центра.	4			№№ 1-8	Опрос, реферат, статья
6.	Управление инфраструктурой открытых ключей Введение в управление PKI. Управление сертификатами. Списки отозванных сертификатов.	4			№№ 1-8	Опрос, реферат, статья
7.	Управление инфраструктурой открытых ключей Протокол OCSP. Сетевой ответчик. Особенности применения КриптоПро OCSP. Управление удостоверяющими центрами. Планирование аварийного восстановления.	4			№№ 1-8	Опрос, реферат, статья
8.	Настройка шаблонов сертификатов. Введение в шаблоны сертификатов. Разработка и создание шаблона сертификатов. Публикация шаблона сертификатов. Управление изменениями в шаблонах сертификатов.	4			№№ 1-8	Опрос, реферат, статья
9.	Настройка выпуска сертификатов	4			№№ 1-8	Опрос,

	Введение в выпуск сертификатов. Ручной выпуск сертификатов. Автоматический выпуск сертификатов.					реферат, статья
10.	Настройка архивирования и восстановления ключей Введение в архивирование и восстановление ключей. Внедрение ручного архивирования и восстановления ключей. Внедрение автоматического архивирования и восстановления ключей.	6			№№ 1-8	Опрос, реферат, статья
11.	Обеспечение конфиденциальности данных Архитектура EFS. Шифрование данных с помощью EFS. Особенности применения КриптоПро EFS.	6			№№ 1-8	Опрос, реферат, статья
12.	Обеспечение конфиденциальности данных Обеспечение конфиденциальности данных. Архитектура EFS. Шифрование данных с помощью EFS. Особенности применения КриптоПро EFS.	4			№№ 1-8	Опрос, реферат, статья
13.	Настройка доверия между организациями Дополнительные вопросы, связанные с иерархией удостоверяющих центров. Настройка ограничений в файле Policy.inf. Возможности квалифицированного подчинения.	4			№№ 1-8	Опрос, реферат, статья
14.	Внедрение смарт-карт Введение в смарт-карты. Выпуск сертификатов для смарт-карт. Внедрение смарт-карт. Применение биометрической идентификации в смарт-картах. Особенности применения КриптоПро WinLogon.	6			№№ 1-8	Опрос, реферат, статья
15.	Защита трафика с применение криптографии Введение в SSL/TLS. Включение SSL/TLS на web-сервере. Особенности применения КриптоПро TLS.	4			№№ 1-8	Опрос, реферат, статья
16.	Защита трафика с применение криптографии Внедрение аутентификации на основе сертификатов. Введение в IPsec. Особенности применения КриптоПро IPsec.	6			№№ 1-8	Опрос, реферат, статья
17.	Настройка защищенной электронной почты Введение в защищенную электронную почту. Настройка защиты для электронного письма. Восстановление секретного ключа для электронной почты.	4			№№ 1-8	Опрос, реферат, статья
ИТОГО		76				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности подготовки реализация компетентностного подхода предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий.

Аудиторная работа включает: лекции, практические занятия, мастер-классы, консультации.

В курсе лекций использованы наглядные, иллюстрированные материалы, обширная информация в табличной и графической формах, а также электронные ресурсы сети Интернет. Разработаны продвинутые лекции (с визуализацией) в формате презентаций, с использованием пакета прикладных программ MS Power Point.

Внеаудиторная работа призвана для формирования и развития профессиональных навыков обучающихся. Самостоятельная работа включает: выполнение домашних заданий, подготовка рефератов, участие в дискуссиях, работа в информационно-образовательной среде. В конце обучения проводится экзамен.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 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 _____ **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	Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. — Пенза : ПГУ, 2018. — 186 с. — ISBN 978-5-907102-51-4. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/162235	
2.	лк, пз, срс	Овчинников, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Овчинников. — Санкт-Петербург : ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/216491	
3.	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	
Дополнительная				
4.	лк, пз, срс	Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/118230	
5.	лк, пз, срс	Исследование методов кодирования и шифрования : учебное пособие / А. П. Алексеев, М. И. Макаров, О. В. Сирант,	URL: https://e.lanbook.com/book/182252	

		С. С. Яковлева ; под редакцией А. П. Алексеева. — Самара : ПГУТИ, 2018. — 102 с. — Текст : электронный // Лань : электронно-библиотечная система. —	
6.	лк, пз, срс	Криптографические методы защиты информации : учебное пособие / составители И. А. Калмыков [и др.]. — Ставрополь : СКФУ, 2015. — 109 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/155280
7.	лк, пз, срс	Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 91 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/163861
8.	лк, пз, срс	Стеганографические и криптографические методы защиты информации : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/90963

7. Материально-техническое обеспечение дисциплины (модуля) «Инфраструктура открытых ключей в СЗИ»

Материально-техническое обеспечение дисциплины включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.rar (Windows, x86).

8.4. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

При проведения лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС http://library.mirea.ru/.

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