

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Баламирзоев Назим Лиодинович

Должность: Ректор

Дата подписания: 30.10.2023 10:36:49

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 Методы и средства криптографической защиты информации

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



подпись

Качаева Г.И.

(ФИО уч. степень, уч. звание)

« 16 » 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)



подпись

Качаева Г.И., к.э.н.

(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)



подпись

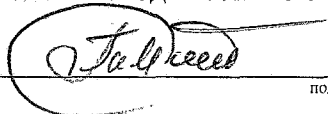
Качаева Г.И., к.э.н.

(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



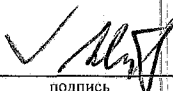
подпись

Исабекова Т.И., к.ф-м.н., доцент

(ФИО уч. степень, уч. звание)

от «18» октября 2021 г.

Декан факультета



подпись

Юсуфов Ш.А.

ФИО

Начальник УО



подпись

Магомаева Э.В.

ФИО

И.о проректора по УР



подпись

Баламирзоев Н.А.

ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Методы и средства криптографической защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности, Математическая логика и теория алгоритма.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Обеспечение ИБ в интеллектуальных системах.

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

В результате освоения дисциплины «Методы и средства криптографической защиты информации» студент должен овладеть следующими компетенциями:

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-10.1.5 знает основные задачи и понятия криптографии
		ОПК-10.1.6 знает модели шифров и математические методы их исследования

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	-		
Лабораторные занятия, час	34		
Самостоятельная работа, час	40		
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)	36		

4.1.Содержание дисциплины (модуля) «Методы и средства криптографической защиты информации»

№ 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: «Нападения и угрозы в компьютерных системах». Ретроспективный анализ развития подходов к разработке средств криптографической защиты информации. Понятия «информация», ее «источники и носители». Информация общедоступная и ограниченного доступа. Категории ценности информации. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; приводится классификация атак. Модели сетевой безопасности и безопасности информационной системы. Информация как объект защиты. Основные задачи обеспечения криптографической защиты информации. Основные методы и средства защиты информации в информационных системах. Анализ угроз информационной безопасности; классификация угроз.	2	-	2	2								
2	Тема: «Введение в криптологию. Основные цели и задачи криптографии». Возникновение и развитие криптографии и криптоанализа. Общие методы криптографии и криптоанализа. Виды конфиденциальной информации и их защита. Способы и средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Взлом криптоалгоритмов. Виды атак на криптографические протоколы. Причины нарушения безопасности информации при ее обработке СКЗИ.	2	-	2	2								
3	Тема «Историческая криптография» Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.	2	-	2	2								

4	Тема: «Математические основы криптографии» Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках.	2	-	2	2								
5	Тема «Симметричное шифрование. Симметричные криптоалгоритмы». Основные понятия, относящиеся к алгоритмам симметричного шифрования. Ключ шифрования. Типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, Линейный и дифференциальный криптоанализ. Алгоритмы DES и тройной DES.	2	-	2	2								
6	Тема: «Симметричное шифрование. Симметричные криптоалгоритмы». Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения. Способы создания псевдослучайных чисел. Стандарт алгоритма симметричного шифрования – AES. Критерии выбора стандарта. Атаки на алгоритмы. Понятие резерва безопасности. Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура раунда алгоритмов Rijndael и RC6.	2	-	2	4								
7	Тема: «Симметричное шифрование. Симметричные криптоалгоритмы». Блочные шифры. DES-алгоритм: история создания, строение, режимы шифрования, применение, характеристики аппаратных и программных реализаций. 3-DES.	2	-	2	2								

8	Тема: «Симметричное шифрование. Симметричные криптоалгоритмы». Алгоритм шифрования ГОСТ-28147. Алгоритмы шифрования FEAL-N и IDEA. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющих в шифртексте искажения открытого текста. Поточковые шифры. Структура. Гаммирование. Основные критерии качества. Синхронные (СПШ) и самосинхронизирующиеся (ССПШ) поточковые шифры. Виды СПШ. Атака на СПШ с помощью вставки символа.	2	-	2	2								
9	Тема: «Алгоритмические проблемы теории чисел». Измерение сложности теоретико-числовых алгоритмов. Полиномиальные алгоритмы. Алгоритм вычисления $a^d \bmod m$. Алгоритм Евклида. Алгоритм решения уравнения $ax + by = 1$. Простые и составные числа. Построение больших простых чисел. Разложение составных чисел на множители. Дискретное логарифмирование. Алгоритмически неразрешимые задачи в криптографии	2	-	2	2								
10	Тема: «Криптография с открытым ключом». Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамала. Криптосистема Рабина. Алгоритмы работы с большими числами.	2	-	2	4								
11	Тема: «Криптография с открытым ключом». Предпосылки появления криптографии с открытым ключом. Схемы шифрования с открытым ключом. Функция Эйлера Основные понятия, относящиеся к криптографии с открытым ключом, а также способы их использования. Обмен ключами. Реализация алгоритма RSA.	2	-	2	4								

12	Тема: «Криптография с открытым ключом». Процедуры шифрования и расшифрования в шифрсистеме Эль-Гамала. Процедура генерации ключей шифрсистемы Эль-Гамала. Работа в режиме подписи. Криптостойкость алгоритма. Преимущества и недостатки систем асимметричного шифрования. Взлом криптосистем с открытым ключом.	2	-	2	2								
13	Тема: «Идентификация и аутентификация». Функции хэширования. Классификация. Функции хэширования без ключа (MDC) и с ключом (MAC). Принципы построения. Функции хэширования Ривеста: MD2, MD4, MD5. Американский стандарт функции хэширования (SHS) и его изменения. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).	2	-	2	2								
14	Тема: «Идентификация и аутентификация». Применение функции хэширования в схемах цифровой подписи и при построении криптосистем. Сильные хэш-функции SHA-1, SHA-2. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC. Контроль целостности данных. Идентификация и аутентификация. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющих в шифртексте искажения открытого текста. Шифрование, создание и проверка цифровой подписи. Использование открытых ключей. Схемы подписи RSA и Рабина. Схема цифровой подписи Эль Гамала и ее модификации.	2	-	2	2								
15	Тема «Хеширование» Криптографические хеш-функции. ГОСТ Р 34.11-2012. DES. AES.	2	-	2	2								

16	Тема: «Стойкость шифра». Определение теоретической стойкости алгоритма. Шифр Вернама для 8-битных символов. Побитный «одноразовый блокнот». Виды атак. Понятие о и практической стойкости шифра. Защита от угроз нарушения целостности информации на уровне содержания. Временная стойкость шифра.	2	-	2	2								
17	Тема: «Электронная подпись» Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10- 2012. DSS. Инфраструктура открытого ключа.	2	-	2	2								
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								

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	Нападения и угрозы в компьютерных системах.	2			№№ 1-14
2	№2	Введение в криптологию. Основные цели и задачи криптографии.	2			№№ 1-14
3	№3	Историческая криптография.	2			№№ 1-14
4	№4	Математические основы криптографии.	2			№№ 1-14
5	№5	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14
6	№ 6	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14
7	№7	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14
8	№8	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14
9	№9	Алгоритмические проблемы теории чисел.	2			№№ 1-14
10	№10	Криптография с открытым ключом.	2			№№ 1-14
11	№11	Криптография с открытым ключом.	2			№№ 1-14
12	№12	Криптография с открытым ключом.	2			№№ 1-14
13	№13	Идентификация и аутентификация.	2			№№ 1-14
14	№14	Идентификация и аутентификация.	2			№№ 1-14
15	№15	Хеширование.	2			№№ 1-14
16	№16	Стойкость шифра.	2			№№ 1-14
17	№17	Электронная подпись.	2			№№ 1-14
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	Нападения и угрозы в компьютерных системах.	2			№№ 1-14	Опрос, реферат, статья
2	Введение в криптологию. Основные цели и задачи криптографии.	2			№№ 1-14	Опрос, реферат, статья
3	Историческая криптография.	2			№№ 1-14	Опрос, реферат, статья
4	Математические основы криптографии.	2			№№ 1-14	Опрос, реферат, статья
5	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14	Опрос, реферат, статья
6	Симметричное шифрование. Симметричные криптоалгоритмы.	4			№№ 1-14	Опрос, реферат, статья
7	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14	Опрос, реферат, статья
8	Симметричное шифрование. Симметричные криптоалгоритмы.	2			№№ 1-14	Опрос, реферат, статья
9	Алгоритмические проблемы теории чисел.	2			№№ 1-14	Опрос, реферат, статья
10	Криптография с открытым ключом.	4			№№ 1-14	Опрос, реферат, статья
11	Криптография с открытым ключом.	4			№№ 1-14	Опрос, реферат, статья
12	Криптография с открытым ключом.	2			№№ 1-14	Опрос, реферат, статья
13	Идентификация и аутентификация.	2			№№ 1-14	Опрос, реферат, статья
14	Идентификация и аутентификация.	2			№№ 1-14	Опрос, реферат, статья
15	Хеширование.	2			№№ 1-14	Опрос, реферат, статья
16	Стойкость шифра.	2			№№ 1-14	Опрос, реферат, статья
17	Электронная подпись.	2			№№ 1-14	Опрос, реферат, статья
ИТОГО		40				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности подготовки реализации 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 продвинутое 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 библиотек е	На кафедре
Основная				
1.		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.		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, С. С. Яковлева ; под редакцией А. П. Алексеева. — Самара : ПГУТИ, 2018. — 102 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/182252	-
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. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой

Мет

Алиева Ж.А.

п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы	Количество изданий	
			В библиотек е	На кафедре
Основная				
1.		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.		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, С. С. Яковлева ; под редакцией А. П. Алексеева. — Самара : ПГУТИ, 2018. — 102 с. — Текст : электронный // Лань : электронно-библиотечная система. —	URL: https://e.lanbook.com/book/182252	-
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	-

8. Материально-техническое обеспечение дисциплины (модуля) «Методы и средства криптографической защиты информации»

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 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/>.

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 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)