Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 06.11.2025 10:20:18
Уникальный программный ключ:
5cf0d6f89e80f49a334f6a4ba58e91f5326b9926

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Программно-аппаратные средства защиты информации
наименование дисциплины по ОПОП

для направления 10.03.01 Информационная безопасность
код и полное наименование специальности

по профилю Безопасность автоматизированных 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 3,4 семестр (ы) 6,7
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению 10.03.01 Информационная безопасность и профилю Безопасность автоматизированных систем.

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

«18» 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 .

[redacted]

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «Программно-аппаратные средства защиты информации» является Формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств, а также навыков и умения в применении знаний для конкретных условий. Развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

Задачи изучения дисциплины: дать знания по концепции обеспечения информационной безопасности компьютерных систем; программно-аппаратным средствам, реализующим отдельные функциональные требования по защите; методам и средствам хранения ключевой информации; методам и средствам ограничения доступа к компонентам вычислительных систем; защите программ от изменения и контролю целостности; задачам и технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.

2.Место дисциплины в структуре ОПОП

Дисциплина «Программно-аппаратные средства защиты информации» относится к блоку 1 (обязательная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Открытые информационные системы, Аппаратные средства вычислительной техники.

Последующими дисциплинами являются: Комплексное обеспечение информационной безопасности автоматизированных систем, Аттестация объектов информатизации по требованиям безопасности информации, Информационная безопасность открытых систем.

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

В результате освоения дисциплины «Программно-аппаратные средства защиты информации» студент должен овладеть следующими компетенциямиОПК-10; ОПК-4.3

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ОПК-10	Способен в качестве технического специалиста принимать участие в	ОПК-10.1.1 - знает программно-аппаратные средства защиты информации в типовых

[redacted]

7	Тема №7: Программно-аппаратные средства обеспечения информационной безопасности.	2	-	2	2								
8	Тема №8: Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчера доступа.	2	-	2	2								
9	Тема №9: Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности.	2	-	2	2								
10	Тема №10: Взаимодействие с общесистемными компонентами вычислительных систем	2	-	2	2								
11	Тема №11: Методы и средства защиты программного обеспечения. Понятие политики безопасности. Описание типовых политик безопасности.	2	-	2	4								
12	Тема №12: Угрозы безопасности компьютерных систем. Модель политики безопасности на основе дискретных компонент АДЕПТ-50.	2	-	2	2								
13	Тема №13: Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	2	-	2	2								
14	Тема №14: Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих	2	-	2	4								
15	Тема №15: Программно-аппаратные средства криптографической защиты информации. Роль и место криптографических методов и средств в обеспечении безопасности компьютерной информации.	2	-	2	2								
16	Тема №16: Основные понятия и процедуры технологии управления криптографическими ключами.	2	-	2	4								
17	Тема №17: Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.	2	-	2	2								

18	Тема №18: Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты. Секретная информация, используемая для контроля доступа: ключи и пароли.	2	-	2	2								
19	Тема №19: Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.	2	-	2	2								
20	Тема №20: Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ.	2	-	2	2								
21	Тема №21: Общее понятие зашиты от копирования. Разновидности задач защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.	2	-	2	2								
22	Тема №22: Привязка программ к гибким магнитным дискам (ГМД). Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы "водяных знаков" и методы "отпечатков пальцев".	2	-	2	2								
23	Тема №23: Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статическое и динамическое изучение. Роль программной и аппаратной среды. Временная надежность (невозможность обеспечения гарантированной надежности).	2	-	2	2								
24	Тема №24: Защита от отладки. Динамическое преобразование кода. Принцип ловушек и избыточного кода. Защита от дизассемблирования. Принцип внешней загрузки файлов. Динамическая модификация программы. Защита от трассировки по прерываниям.	2	-	2	2								
25	Тема №25: Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий. Защита от разрушающих программных воздействий.	2	-	2	2								

26	Тема №26: Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.	2	-	2	2								
27	Тема №27: Понятие изолированной программной среды.	2	-	2	2								
28	Тема №28: Программные средства антивирусной защиты: основные характеристики, принципы построения и применения.	2	-	2	4								
29	Тема №29: Построение изолированной программной среды. Модель компьютерной системы.	2	-	2	2								
30	Тема №30: Понятие монитора безопасности. Обеспечение гарантий выполнения политики безопасности.	2	-	2	2								
31	Тема №31: Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.	2	-	2	4								
32	Тема №32: Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.	2	-	2	2								
33	Тема №33: Обеспечение информационной безопасности компьютерных сетей. Программно-аппаратные средства защиты информации в сетях передачи данных.	2	-	2	4								
34	Тема №34: Межсетевые экраны. Свойства экранирующего субъекта. Классификация требований к классам межсетевых экранов.	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)		экзамен				Зачет/ зачет с оценкой/ экзамен				Зачет/ зачет с оценкой/ экзамен			
Итого		68	-	68	80								

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	Повышение стойкости парольной системы идентификации на основе применения метода разделения знаний (пароля).	6			№№ 1-7
2.	№2	Демонстрация принципа аутентификации с нулевым разглашением на основе схемы Гиллоу-Куискуотера	6			№№ 1-7
3.	№ 3-4	Настройка параметров аутентификации Windows XP	6			№№ 1-7
4.	№5-6	Формирование учетной записи с ограниченными правами и установить для нее пароль (операционная система Windows XP).	6			№№ 1-7
5.	№7-8	Настройка брандмауэра Windows XP (добавить рограмму в список исключений по указанию преподавателя).	6			№№ 1-7
6.	№9	Установка режима работы с документами MS Word при котором запрещается бесконтрольная обработка всех макросов.	6			№№ 1-7
7.	№10	Установка парольной защиты на документ MS Word, предотвращающую несанкционированное изменение содержания документа.	6			№№ 1-7
8.	№11	Зашифрование (расшифрование) сообщения (криптограммы)	6			№№ 1-7
9.	№12	Рассчитать требуемую мощность пространства паролей, обеспечивающую требуемый уровень надежности парольной защиты (данные по заданию преподавателя).	6			№№ 1-7
10.	№13-14	Проверка потенциальных местах записей вредоносного программного обеспечения в системном реестре операционной системы Windows 2000 (XP) [Найдите ключ Userinit (REG_SZ) и проверьте его содержимое]	6			№№ 1-7
11.	№15	Активизация механизма регистрации и аудита с помощью	4			№№ 1-7

		оснастки «Локальные политики безопасности» системы безопасности ОС Windows				
12.	№16-17	Создание VPN-подключение средствами ОС Windows	4			№№ 1-7
ИТОГО			68			

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.	Программно-аппаратные средства разграничения доступа к компьютерной информации.	2			№№ 1-7	Опрос, реферат, статья
2.	Основы защиты компьютерной информации от несанкционированного доступа.	2			№№ 1-7	Опрос, реферат, статья
3.	Понятие идентификации и аутентификации субъекта.	2			№№ 1-7	Опрос, реферат, статья
4.	Классификация средств хранения ключей и идентифицирующей информации.	2			№№ 1-7	Опрос, реферат, статья
5.	Стандарты информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья
6.	Основные категории требований к программной и программно- аппаратной реализации средств обеспечения информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья
7.	Программно-аппаратные средства обеспечения информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья
8.	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.	2			№№ 1-7	Опрос, реферат, статья
9.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите.	2			№№ 1-7	Опрос, реферат, статья
10.	Взаимодействие с общесистемными компонентами вычислительных систем	2			№№ 1-7	Опрос, реферат, статья

11.	Методы и средства защиты программного обеспечения.	4			№№ 1-7	Опрос, реферат, статья
12.	Угрозы безопасности компьютерных систем.	2			№№ 1-7	Опрос, реферат, статья
13.	Методы и средства ограничения доступа к компонентам вычислительных систем.	2			№№ 1-7	Опрос, реферат, статья
14.	Методы и средства хранения ключевой информации.	4			№№ 1-7	Опрос, реферат, статья
15.	Программно-аппаратные средства криптографической защиты информации.	2			№№ 1-7	Опрос, реферат, статья
16.	Основные понятия и процедуры технологии управления криптографическими ключами.	4			№№ 1-7	Опрос, реферат, статья
17.	Аппаратные и программно-аппаратные средства криптозащиты данных.	2			№№ 1-7	Опрос, реферат, статья
18.	Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.	2			№№ 1-7	Опрос, реферат, статья
19.	Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.	2			№№ 1-7	Опрос, реферат, статья
20.	Несанкционированное копирование программ как тип НСД.	2			№№ 1-7	Опрос, реферат, статья
21.	Общее понятие зашиты от копирования.	2			№№ 1-7	Опрос, реферат, статья
22.	Привязка программ к гибким магнитным дискам, к жестким магнитным дискам.	2			№№ 1-7	Опрос, реферат, статья
23.	Понятие изучения и обратного проектирования ПО.	2			№№ 1-7	Опрос, реферат, статья
24.	Защита от отладки.	2			№№ 1-7	Опрос, реферат, статья
25.	Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий.	2			№№ 1-7	Опрос, реферат, статья
26.	Вирусы как особый класс разрушающих программных воздействий.	2			№№ 1-7	Опрос, реферат, статья
27.	Понятие изолированной программной среды.	2			№№ 1-7	Опрос, реферат, статья
28.	Программные средства антивирусной защиты: основные характеристики, принципы	4			№№ 1-7	Опрос, реферат, статья

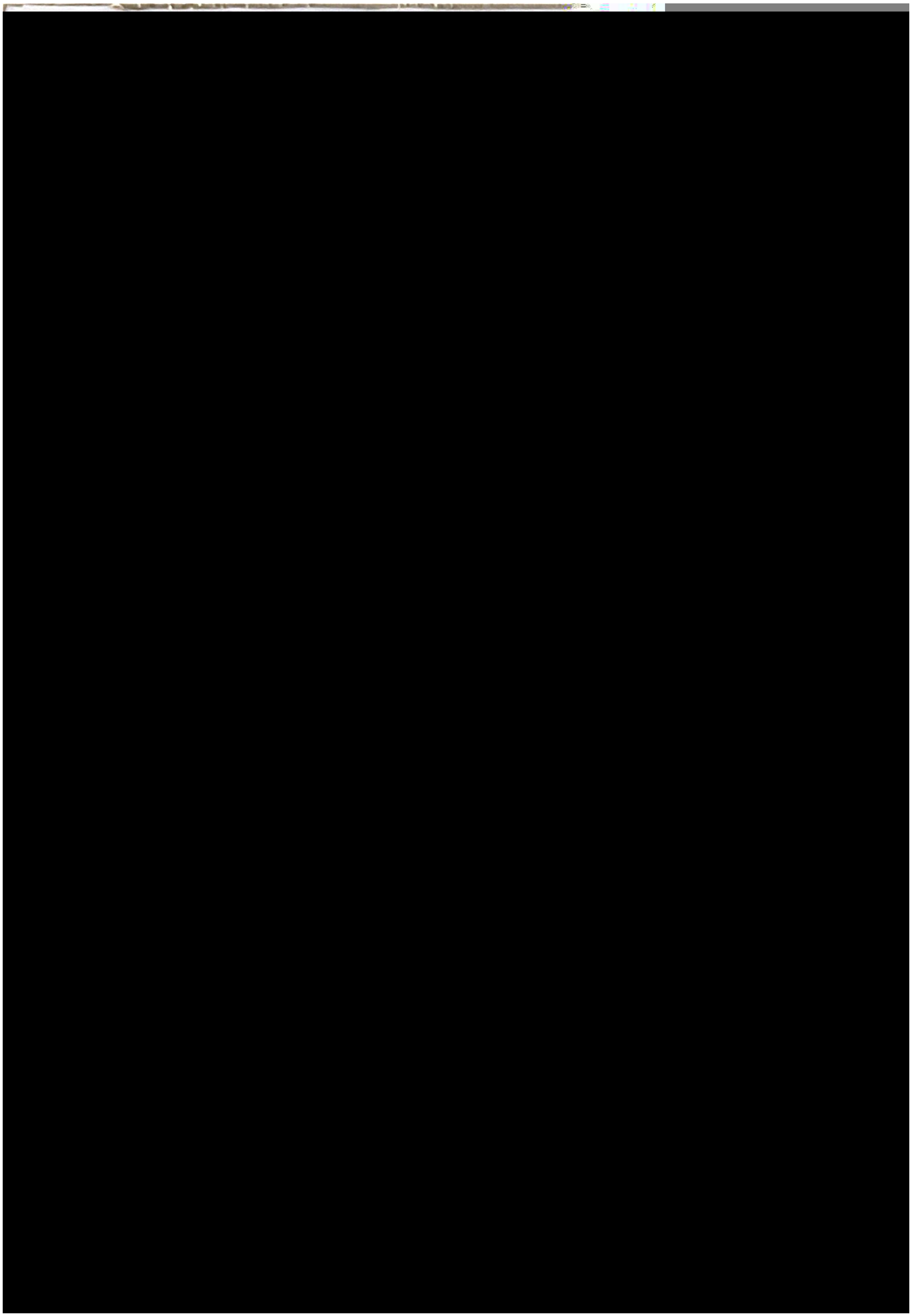
ния и применения.					
ение изолированной программной компьютерной системы.	2			№№ 1-7	Опрос, реферат, статья
монитора безопасности.	2			№№ 1-7	Опрос, реферат, статья
енерации изолированной мной среды при проектировании мов гарантированного поддержания и безопасности.	4			№№ 1-7	Опрос, реферат, статья
безопасного взаимодействия в КС.	2			№№ 1-7	Опрос, реферат, статья
ение информационной безопасности терных сетей.	4			№№ 1-7	Опрос, реферат, статья
евые экраны.	2			№№ 1-7	Опрос, реферат, статья
	80				

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению 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 [redacted]



7. Материально-техническое обеспечение дисциплины (модуля) «Программно-аппаратные средства 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).

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

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)