

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 06.11.2025 10:16:40
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 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



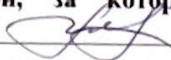
Качасва Г.И., к.э.н.

подпись

(ФИО уч. степень, уч. звание)

« 18 » 09 2021г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)



Качасва 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)



Качасва Г.И., к.э.н.

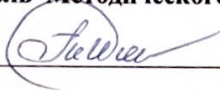
подпись

(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

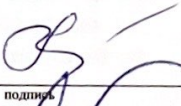


Юсуфов Ш.А.

подпись

ФИО

Начальник УО

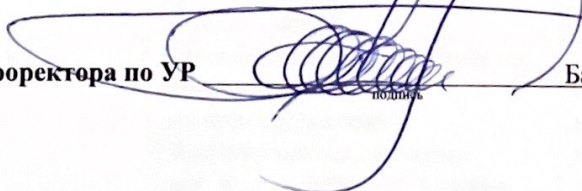


Магомаева Э.В.

подпись

ФИО

И.о проректора по УР



Баламирзоев Н.Л.

подпись

ФИО

1. Цели и задачи освоения дисциплины.

Целями освоения дисциплины (модуля) «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).

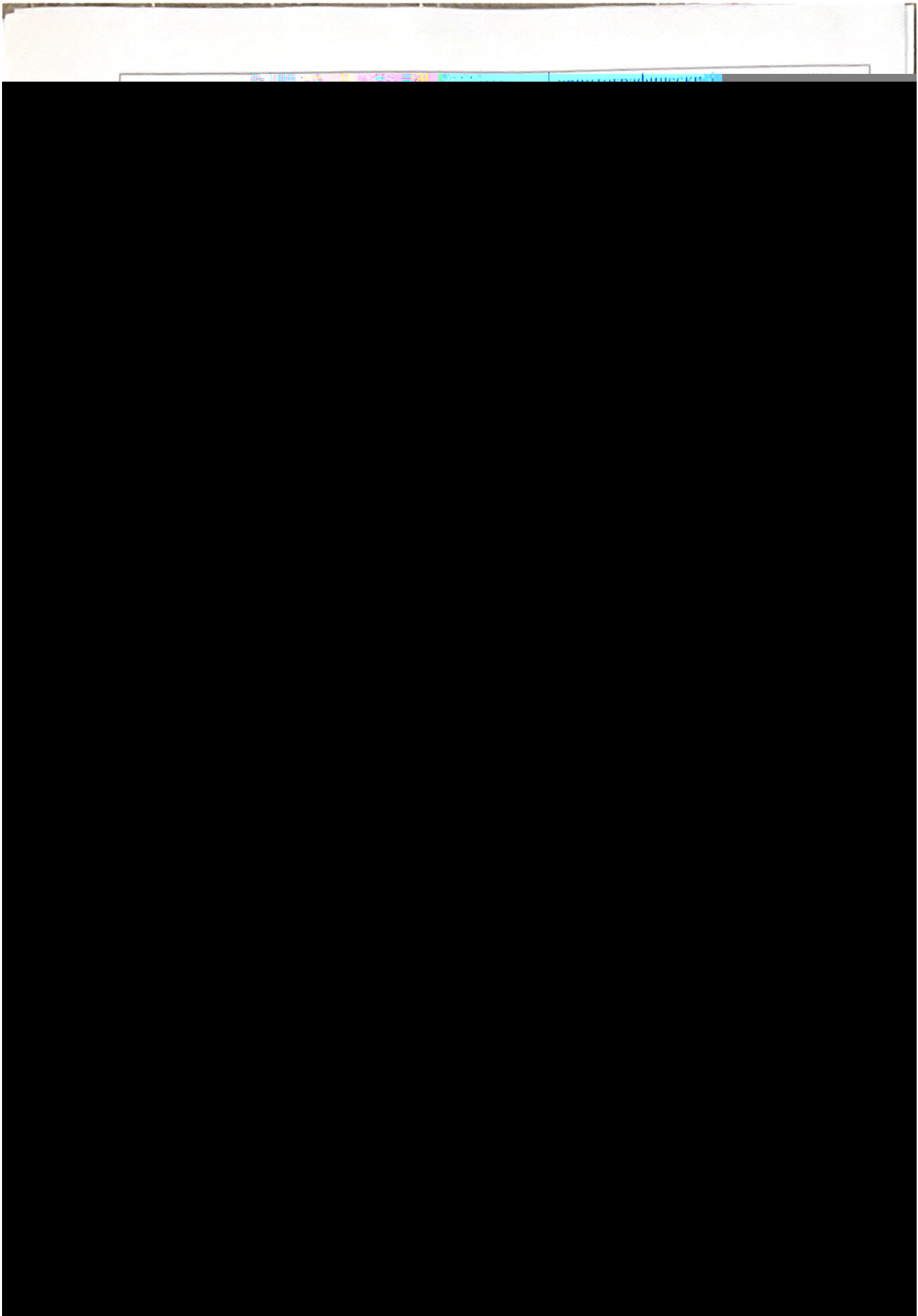
Предшествующими дисциплинами, формирующими начальные знания, являются: Открытые информационные системы, Аппаратные средства вычислительной техники.

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 компетенциями ОПК-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 формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1 - знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях
		ОПК-10.2.1 - умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности
ОПК-4.3	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и	ОПК-4.3.1. Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации.
		ОПК-4.3.1. Умеет использовать программные, программно-аппаратные (в том числе



4.1. Содержание дисциплины (модуля) «Программно-аппаратные средства защиты информации»

4.1.Содержание дисциплины (модуля) «Программно-аппаратные средства 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 №1: Введение. Цели и задачи дисциплины. Основные понятия и определения в области защиты компьютерной информации. Современная ситуация в области защиты компьютерной информации. Программно-аппаратные средства разграничения доступа к компьютерной информации.	2	-	2	2										
2	Тема № 2: Основы защиты компьютерной информации от несанкционированного доступа. Основные термины и определения в области защиты компьютерной информации от НСД. Основные принципы и направления защиты от НСД. Формальные модели управления доступом.	2	-	2	2										
3	Тема № 3: Понятие идентификации и аутентификации субъекта. Алгоритмы аутентификации пользователей. Секретная информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи.	2	-	2	2										
4	Тема № 4: Классификация средств хранения ключей и идентифицирующей информации. Магнитные диски прямого доступа. Магнитные и интеллектуальные. Средство TouchMemory.	2	-	2	2										
5	Тема №5: Стандарты информационной безопасности. Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.	2	-	2	2										
6	Тема №6: Основные категории требований к программной и программно- аппаратной реализации средств обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий производства.	2	-	2	2										

[illegible]

ебнелх
пнлнмх

* - 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

№ 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 установка для нее пароль (операционная система Windows XP).	6			№№ 1-7	
5.	№7-8	Настройка брандмауэра Windows XP (добавить программу 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 мест 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 защиты 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

	построения и применения.						*
29.	Построение изолированной программной среды.	2				№№ 1-7	Опрос, реферат, статья
30.	Модель компьютерной системы.						
31.	Понятие монитора безопасности.	2				№№ 1-7	Опрос, реферат, статья
	Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.	4				№№ 1-7	Опрос, реферат, статья
32.	Модели безопасного взаимодействия в КС.	2				№№ 1-7	Опрос, реферат, статья
33.	Обеспечение информационной безопасности компьютерных сетей.	4				№№ 1-7	Опрос, реферат, статья
34.	Межсетевые экраны.	2				№№ 1-7	Опрос, реферат, статья
ИТОГО		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 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

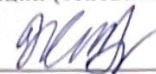
Оценочные средства приведены в ФОС (Приложение А)

7. Учебно-методическое и информационное обеспечение дисциплины

Программно-аппаратные средства защиты информации

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	Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/180093	
2.	лк, пз, срс	Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/156494	
3.	лк, пз, срс	Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система.	URL: https://e.lanbook.com/book/130184	
Дополнительная				
4.	лк, пз, срс	Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Д. В. Фомин. — Саратов : Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/110329.html	
5.	лк, пз, срс	Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 21 с. — ISBN 978-5-906953-22-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/98199.html	
6.	лк, пз, срс	Методы и средства обеспечения программно-аппаратной защиты информации : научно-техническое издание / А. И. Астайкин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 с. — ISBN 978-5-9515-0305-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/60959.html	
7.	лк, пз, срс	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации / составители И. А. Денисов. — Москва : Московский технический университет связи и информатики, 2016. — 31 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].	URL: https://www.iprbookshop.ru/61529.html	

8 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 dumptasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumptasn1.rar (Windows, x86).

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/>.

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 06.09.2015 № 1009/15-ОС

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

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)