Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Безопасность вычислительных сетей
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, очно-заочная 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) Машинно-зависимые языки программирования

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

«18» 09 2021г.

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

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)

_____ Качаева Г.И., к.э.н.
подпись (ФИО уч. степень, уч. звание)

«20» 09 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от 18.10 2021 года, протокол № 1.

Председатель Методического совета факультета КТВТиЭ

_____ Исабекова Ш.А.
подпись (ФИО уч. степень, уч. звание)

«18» 10 2021г.

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.

Целью дисциплины «Безопасность вычислительных сетей» является изучение принципов и методов защиты информации в сетях, изучение принципов и алгоритмов обеспечения и построения безопасных сетей ЭВМ.

Задачи дисциплины:

- Изучение основных угроз в сетях ЭВМ и методов противодействия им;
- Овладения механизмами построения систем безопасности сетей ЭВМ;
- Изучение мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- Изучить защищенные протоколы и межсетевые экраны.

2.Место дисциплины в структуре ОПОП

Дисциплина « Безопасность вычислительных сетей» относится к блоку 1 (Часть, формируемая участниками образовательных отношений).

Предшествующими дисциплинами, формирующими начальные знания, являются: Аппаратные средства вычислительной техники, Операционные системы, Безопасность систем баз данных, Основы информационной безопасности, Базы данных и экспертные системы, знание основ курса " Основы управления информационной безопасностью".

Последующими дисциплинами являются: Информационная безопасность открытых систем, Комплексное обеспечение информационной безопасности автоматизированных систем, Методы оценки безопасности компьютерных систем.

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

В результате освоения дисциплины «Безопасность вычислительных сетей» студент должен овладеть следующими компетенциями:

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1. Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации. ПК-1.2. Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации. ПК-1.3. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации
ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения	ПК-2.1. Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования. ПК-2.2. Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации.

	профессиональных задач	ПК-2.3. Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения ПК-3.2 Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4.1 Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе ПК-4.2 Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия ПК-4.3 Владеет навыками разработки руководящих документов по защите информации в организации

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	7/252	7/252	-
Семестр	6,7	6,7	-
Лекции, час	68	34	-
Практические занятия, час	-	-	-
Лабораторные занятия, час	68	34	-
Самостоятельная работа, час	80	148	-
Курсовой проект (работа), РГР, семестр	-	-	-
Зачет (при заочной форме **4 часа** отводится на контроль)	6 семестр	6 семестр	-
Часы на экзамен (при очной, очно-заочной формах **1 ЗЕТ – 36 часов**, при заочной форме **9 часов** отводится на контроль)	**36 (7 семестр)**	**36 (7 семестр)**	-

4.1.Содержание дисциплины (модуля) « Технология построения защищенных автоматизированных систем»

№ 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.	**Лекция №1. Введение в сетевую безопасность** 1. Основные понятия и определения 2. Нейтрализация угроз. Области сетевой безопасности 3. Общие рекомендации по сетевой безопасности. 4. Типы атак.	2	-	1	2	1	-	1	4	-	-	-	-
2.	**Лекция №2 Аудит информационной безопасности** 1. Основные виды аудита безопасности 2. Экспертный аудит 3. Инструментальный анализ защищенности. **4.** Основные этапы работ при проведении аудита.	2	-	1	2	1	-	1	4	-	-	-	-
3.	**Лекция №3 Протоколы сетевой аутентификации. Модели разграничения доступа. Вредоносное программное обеспечение.** 1. Локальная аутентификация Windows 2. Протоколы сетевой аутентификации.	2	-	1	2	1	-	1	4	-	-	-	-
4.	**Лекция №4 Системы предотвращения утечек информации. Системы анализа трафика. Файрвол веб-приложений** 1. DLP-системы. 2. DMZ –системы 3. DPI- системы. 4. WAF-системы.	2	-	1	2	1	-	1	4	-	-	-	-
5.	**Лекция №5 Системы обнаружения и предотвращения вторжений (ISD/IPS)** 1. Что такое системы обнаружения вторжений (IDS). 2. Сетевые ISD (NIDS) 3. Проблемы NIDS 4. Системы предотвращения вторжений (IPS).	2	-	1	2	1	-	1	4	-	-	-	-

6.	**Лекция №6 Угрозы безопасности на канальном уровне 2** 1. Атака на таблицу MAC. 2. Атаки на сети VLAN. 3. Атаки, связанные с DHCP. 4. ARP атаки. **5.** Атаки с подменой адреса.	2	-	1	2	1	-	1	4				
7.	**Лекция № 7** Настройка параметров безопасности коммутатора cisco. 1. Защита не используемых портов. 2. Нейтрализация атак таблицы MAC-адресов. 3. Ограничение и изучение MAC-адресов. **4.** Режимы нарушения безопасности порта.	2	-	1	2	1	-	1	4				
8.	**Лекция №8 Обеспечение безопасности сетевых устройств** 1. Защита доступа к устройствам. 2. Назначение административных ролей. 3. Простой протокол сетевого управления SNMP.	2	-	1	2	1	-	1	4				
9.	**Лекции №9 Межсетевые экраны** 1. Определение типов межсетевых экранов. 2. Разработка конфигурации межсетевого экрана. 3. Построение набора правил межсетевого экрана. Выявление различий между межсетевыми экранами различных типов	2	-	1	2	1	-	1	4				
10.	**Лекция 10 Дополнительные возможности Wireshark для графического представления получаемых результатов.** 1. Конечные точки и сетевые диалоги. 2. Выявление наиболее активных сетевых узлов с помощью конечных точек и диалогов	2	-	1	2	1	-	1	4				

11.	**Лекция №11 Методы сбора информации.** 1. Общедоступные сайты, которые можно использовать для сбора информации о целевом домене. Использование общих ресурсов. 2. Информация о регистрации домена. 3. Анализ DNS. 4. Информация о маршруте. 5. Использование поисковой системы.	2	-	1	2	1	-	1	4				
12.	**Лекция № 12: Уязвимости по приложениям** 1. SSTI. 2. XXE-атака. 3. XSS-атаки. 4. Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet .xssFilter.	2	-	1	2	1	-	1	4				
13.	**Лекция №13: Атака на сервер компьютерной сети** 1. SSRF атака **2.** Компрометация сервера	2	-	1	2	1	-	1	4				
14.	**Лекция №14: Способы обхода авторизации** 1. BruteForce. 2. SQL инъекции. 3. Cookie.	2	-	1	2	1	-	1	4				
15.	**Лекция №15: Sql инъекции** 1. Принцип атаки внедрения SQL. 2. Типы SQLi. 3. Защита от SQLi. 4. Классические атаки. 5. Комментирование, Манипуляции со строками, Обход аутентификации. 6. Union injection.	2	-	1	2	1	-	1	6				

16.	**Лекция №16 Sql инъекции** 1. Последовательные запросы 2. Error-Based 3. Слепые инъекции 4. Условные выражения 5. Boolean-based 6. Time Based SQL-injection 7. Stacked Query Based SQL-injections 8. JSQ injection.	2	-	1	4	1	-	1	6				
17.	**Лекция №17: Защита от SQL-инъекций** 1. Функция mysql(i)_real_escape_string 2. Приведение к числу 3. Использование анализатора sqlmap.	2	-	1	4	1	-	1	6				
	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 1 аттестация 1-5 тема 2 аттестация 6-10 тема 3 аттестация 11-15 тема							
	Форма промежуточной аттестации (по семестрам)	зачет				зачет							
Итого за 6 семестр		34	-	34	40	17	-	17	74				
18.	**Лекция №18 Алгоритмы взлома корпоративной сети** 1. захват учетных записей 2. атака протокола отладки Java Debug Wire Protocol 3. веб-уязвимости 4. Социальная инженерия.	4	-	4	4	2	-	2	8				
19.	**Лекция № 19: Анализ защищённости веб-приложений** 1. Методология тестирования на проникновение: Метод черного ящика (black box), Метод белого ящика (white box), Метод серого ящика (gray box) 2. Анализ защищённости веб-приложений путём внешних проверок (автоматизированных и ручных). 3. Этапы теста на проникновение: 4. Тестирование на проникновение с помощью Burp 5. Nikto – сканер веб-серверов 6. NSLOOKUP – утилита для поиска DNS-серверов	4	-	4	4	2	-	2	8				

20.	**Лекция № 20: Инструменты Kali Linux.** 1. Разведка сайтов. Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster. 2. dirsearch —инструмент командной строки, предназначенный для брут-форса (поиска путём полного перебора) директорий и файлов в веб-сайтах. 3. DVCS-Ripper 4. SQLmap 5. WPScan — это сканер уязвимостей WordPress.	4
21.	**Лекция № 21: Методы сканирования и уклонения в Kali Linux** 1. Описание метода обнаружения цели. 2. Как с помощью инструментов Kali Linux распознать целевую машину. 3. Шаги, которые необходимо выполнить для поиска операционных систем целевых машин (получение отпечатков операционной системы). 4. Автоматическое сканирование с помощью Striker. 5. Сокрытие с помощью Nipe. 6. Сканирование nmap. 7. Sql map 8. NetCat	4
22.	**Лекция № 22: Инструментальные средства командной строки для анализа пакетов**	2
23.	**Лекция № 23: Процесс выявления и анализа критических недостатков безопасности в Kali Linux**	4
24.	**Лекция № 24: Python для тестирования на проникновение** 1. Понимание сокетов и создание TCP-сервера 2. Создание TCP-клиента 3. Разработка сканера Nmap	4
25.	**Лекция № 25: Исследование сетей с Python** 1. Сканер сети библиотеки scapy 2. Использование веб-библиотек. Взаимодействие с веб-сервисами -библиотека urllib2. 3. Форензика с Python 4. Библиотека requests 5. Пакеты lxml и BeautifulSoup.	4

-	4	4	2	-	2	8				
-	4	4	2	-	2	8				
-	2	4	1	-	1	8				
-	4	4	2	-	2	8				
-	4	4	2	-	2	8				
-	4	6	2	-	2	8				

26.	**Лекция № 26: Безопасность беспроводных сетей.** 1. WEP-атаки на конфиденциальность проводных сетей 2. Протоколы WPA и AES 3. Заблуждения о безопасности беспроводной сети 4. Беспроводные атаки и защита от них 5. Проектирование безопасной сети с помощью беспроводной связи.	4	-	4	6	2	-	2	10				
Итого за 7 семестр		34	-	34	40	17	-	17	74	-	-	-	-
Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)		Входная конт.работа 1 аттестация 18-20 тема 2 аттестация 21-23 тема 3 аттестация 24-25 тема				Входная конт.работа 1 аттестация 18-20 тема 2 аттестация 21-23 тема 3 аттестация 24-25 тема							
Форма промежуточной аттестации (по семестрам)		Экзамен (36ч)				Экзамен (36ч)							
Итого		**68**	**-**	**68**	**80**	**17**	**-**	**17**	**148**	**-**	**-**	**-**	**-**

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	Нейтрализация угроз.	2	1	-	№№ 1-8
2.	2	Аудит информационной безопасности.	2	1	-	№№ 1-8
3.	3	Локальная аутентификация Windows.	2	1	-	№№ 1-8
4.	4	DLP-системы. DMZ –системы. DPI- системы. WAF-системы	2	1	-	№№ 1-8
5.	5	Системы обнаружения и предотвращения вторжений	2	1	-	№№ 1-8
6.	6	Угрозы безопасности на уровне 2	2	1	-	№№ 1-8
7.	7	Настройка параметров безопасности коммутатора	2	1	-	№№ 1-8

		cisco.				
8.	8	Простой протокол сетевого управления SNMP.	2	1	-	№№ 1-8
9.	9	Межсетевые экраны.	2	1	-	№№ 1-8
10.	10	Анализатор протоколов Wireshark	2	1	-	№№ 1-8
11.	11	Утилита NSLOOKUP	2	1	-	№№ 1-8
12.	12	Уязвимости по приложениям.	2	1	-	№№ 1-8
13.	13	Уязвимости по приложениям.	2	1	-	№№ 1-8
14.	14,	Способы обхода авторизации	2	1	-	№№ 1-8
15.	15,16	Sql инъекции	2	1	-	№№ 1-8
16.	17	Защита от SQL-инъекций	2	1	-	№№ 1-8
Итого:			34	17	-	№№ 1-8
17.	18	Анализ защищённости веб-приложений	8	4	-	№№ 1-8
18.	19,20	Инструменты Kali Linux	10	5	-	№№ 1-8
19.	21,22	Инструментальные средства командной строки для анализа пакетов.	8	4	-	№№ 1-8
20.	23, 24	Python для тестирования на проникновение	8	4	-	№№ 1-8
ИТОГО			**34**	**17**		

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	1	4	5	6	7
1.	Нейтрализация угроз. Области сетевой безопасности.	2	6	-	№№ 1-8	Опрос, реферат, статья
2.	Экспертный аудит	2	6	-	№№ 1-8	Опрос, реферат, статья
3.	Протоколы сетевой аутентификации	2	6	-	№№ 1-8	Опрос, реферат, статья
4.	WAF-системы	4	6	-	№№ 1-8	Опрос, реферат, статья
5.	Сетевые ISD (NIDS)	4	6	-	№№ 1-8	Опрос, реферат, статья

6.	Режимы нарушения безопасности порта.	4	6	-	№№ 1-8	Опрос, реферат, статья
7.	Защита доступа к устройствам.	2	6	-	№№ 1-8	Опрос, реферат, статья
8.	Выявление различий между межсетевыми экранами различных типов.	4	6	-	№№ 1-8	Опрос, реферат, статья
9.	Конечные точки и сетевые диалоги.	4	6	-	№№ 1-8	Опрос, реферат, статья
10.	Информация о регистрации домена.	2	6	-	№№ 1-8	Опрос, реферат, статья
11.	Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet .xssFilter.	4	6	-		
12.	Атака на сервер компьютерной сети	4	6	-		
13.	Комментирование, Манипуляции со строками, Обход аутентификации.	4	6	-		
14.	Слепые инъекции.	4	6	-		
15.	Защита от SQL-инъекций	4	6	-		
16.	Захват учетных записей.	4	6	-		
17.	Этапы теста на проникновение.	4	6	-		
18.	Разведка сайтов.	2	6	-		
19.	Описание метода обнаружения цели.	2	6	-		
20.	Инструментальные средства командной строки для анализа пакетов.	4	6	-		
21.	Создание TCP-клиента.	4	8	-		
22.	Python для тестирования на проникновение.	4	6	-		
23.	Исследование сетей с Python.	4	8	-		
24.	WEP-атаки на конфиденциальность проводных сетей.	2	6	-		
ИТОГО		**80**	**148**	-		

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 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)

Зав. библиотекой _____ *Алиева Ж.А.*

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

№п/п	Виды занятий	Комплект необходимойучебной литературы подисциплине	Автор(ы)	Издательство игод издания	Количество экземпляров	
					В библио-теке	На каф ед - ре
1	2	3	4	5	6	7
ОСНОВНАЯ						
1	КР,СР	Сети ЭВМ и телекоммуникации. Архитектура и организация: учебное пособие / С. С. Гельбух. — Санкт-Петербург: Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текс: электронный // Лань: электронно-библиотечная система.	Гельбух, С. С.	Лань, 2019.	URL: https://e.lanbook.com/book/118646	
2	КР,СР	Безопасность сетей ЭВМ: учебное пособие / Ю. И. Синицын, Е. И. Ряполова. — Оренбург: ОГУ, 2017. — 189 с. — ISBN 978-5-7410-1886-6. — Текст : электронный // Лан : электронно-библиотечная система. —		Оренбург: ОГУ, 2017	URL: https://e.lanbook.com/book/110613	
3	ЛК, СР, ЛБ	Основы построения компьютерных сетей: учебное пособие / М. В. Левин, И. А. Ушаков, А. Ю. Цветков, П. А. Исаченков. — Санкт-Петербур: СПбГУТ им. М.А. Бонч-Бруевича, 2016. — 55 с. — Текст: электронный // Лань: электронно-библиотечная система.	М. В. Левин, И. А. Ушаков, А. Ю. Цветков, П. А. Исаченков.	Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016.	URL: https://e.lanbook.com/book/180098	
4	ЛК, СР, ЛБ	Компьютерные сети. Анализ и диагностика: учебное пособие / С. П. Борисов. — Москва: РТУ МИРЭА, 2021 — Часть 1 — 2021. — 67 с. — Текст:электронный //Лань: электронно-библиотечная система.	Борисов, С. П.	Москва : РТУ МИРЭА, 2021	URL: https://e.lanbook.com/book/176562	
5	ЛК, СР	Безопасность сетей ЭВМ: методические указания / А. Г. Лютов, Н. Н. Чернышев. — Москва: РТУ МИРЭА, 2021. — 83 с. — Текст: электронный //Лань: электронно-библиотечная система.	Лютов, А. Г.	Москва : РТУ МИРЭА, 2021.	URL: https://e.lanbook.com/book/182523	
6	ЛК, СР	Основы локальных компьютерных сетей: учебное пособие для вузов / А. Н. Сергеев. — 3-е изд., стер. — Санкт-Петербург: Лань, 2021. — 184 с. — ISBN 978-5-8114-6855-3. — Текст: электронный // Лань:	Сергеев, А. Н.	Санкт-Петербург : Лань, 2021.	URL: https://e.lanbook.com/book/152651	-

		электронно-библиотечная система.				
ДОПОЛНИТЕЛЬНАЯ						
7	ЛК, СР	Ракитин, Р. Ю. Компьютерные сети: учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул: АлтГПУ, 2019. — 340 с. — ISBN 978-5-.88210-942-3. — Текст: электронный // Лань: электронно-библиотечная система.	Ракитин, Р. Ю.	Барнаул: АлтГПУ, 2019.	URL: https://e.lanbook.com/book/139182	-
8	ЛК, СР	Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст: электронный // Лань: электронно-библиотечная систем.	Краковский, Ю. М.		URL: https://e.lanbook.com/book/156401	

8. Материально-техническое обеспечение дисциплины (модуля) « Технология построения защищенных автоматизированных систем»

Материально-техническое обеспечение дисциплины « Технология построения защищенных автоматизированных систем» включает:

- библиотечный фонд (учебная, учебно-методическая, справочная техническая литература, техническая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет;
- аудитории, оборудованные проекционной техникой.

Для проведения лекционных занятий используется лекционный зал кафедры ИБ, обору-дованный проектором (ViewSonic PJD- 6221 (DLP 2700 LumensXGA (1024x768) 2800:1/2kgAudioin/aut,BrilliantColour.), интерактивной доской (Smart Technologies Smart Board V280 и моноблок Asus V2201-BUK (2201-BC022M) – компьютерный зал №6.Для проведения лабораторных занятий используются компьютерные классы кафедры Информационной безопасности (компьютерные залы №5, 6), оборудованные современными персональными компьютерами с соответствующим программным обеспечением.

- ауд. № 300- компьютерный зал:

ПЭВМ в сборе: ПЭВМ в сборе: CPU AMD a4-4000-3,0GHz/A68HM-k (RTL) Sosket FM2+/DDR3 DIMM 4Gb/HDD 500Gb Sata/DVD+RW/Minitover 450BT/20,7”ЖК монитор 1920x1080 PHILIPS D-Sub комплект-клавиатура, мышь USB. – 6 шт;

Сист.блок от компмютера IntelPentium(R)4 CPU3000GHzDDR 2048Mb/HDD160Gb DVDRW..мон-р от ком-ра персон.в сост.2048/250Gb Ком-р IntelCel-nCPU2,8 GHz/2048Mb/160Gb…монитор от компьютера Int/ Pentium

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

Интерактивнаядоска Smart Technologies Smart Board V280.

Проектор ViewSonicPJD- 6221 (DLP 2700 LumensXGA (1024x768) 2800:1/2kgAudioin/aut,BrilliantColour.Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

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