МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждениевысшего образования
«Дагестанский государственный университет»

Колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.01.04. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ.

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	*10.02.05.Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваивается ППССЗ:	*основное общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

Махачкала - 2022

Рабочая программа дисциплины «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» разработана на основе требований ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем от 09.12.2016 N1553 для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Организация-разработчик: колледж федерального государственного бюджетного образовательного учреждение высшего образования «Дагестанский государственный университет» (Колледж ДГУ).

Разработчики:
Магомедова Карина Камильевна - заведующая кафедрой специальных дисциплин Колледжа ДГУ, к.ю.н., доцент
Сайгитмагомедова Хадижат Садрутдиновна - преподаватель кафедры информационного права и информатики Юридического института ДГУ.

Рецензент:

Исмиханов З.Н. – к.э.н., доцент, зав. каф. информационных систем и технологий программирования факультета ИиИТ ДГУ

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин Колледжа ДГУ

Протокол № 8 от «30» 04 2022г.

Зав. кафедрой _____/Магомедова К.К./
подпись

Утверждена на заседании учебно-методического совета колледжа ДГУ

Ст. методист _____/Шамсутдинова У.А./

Рабочая программа дисциплины согласована с учебно-методическим управлением «31» 03 2022г. _____
подпись

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Эксплуатация автоматизированных систем в защищенном исполнении

1.1. Область применения программы

Рабочая программа дисциплины «Эксплуатация автоматизированных систем в защищенном исполнении» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05. Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.
Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Эксплуатация автоматизированных систем в защищенном исполнении» относится к профессиональному модулю «Эксплуатация автоматизированных систем в защищенном исполнении» профессионального цикла ППССЗ.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Содержание программы учебной дисциплины «Эксплуатация автоматизированных систем в защищенном исполнении» направлено на достижение следующей цели:

- обеспечить знание теоретических и практических основ в организации и функционировании компьютерных сетей и телекоммуникаций, умение применять в профессиональной деятельности распределенные данные, прикладные программы и ресурсы сетей.

Задачи дисциплины:

- формирование теоретических и практических основ применения компьютерных сетей;
- сформировать навыки работы в глобальной сети;
- научить использовать аппаратные, программные и информационные ресурсы сетей для достижения профессиональных целей;
- научить работе с сетевым программным обеспечением.

Освоение содержания учебной дисциплины «Эксплуатация автоматизированных систем в защищенном исполнении» обеспечивает достижение студентами следующих результатов:

Общие компетенции

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 09. Использовать информационные технологии в профессиональной деятельности.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Профессиональные компетенции

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

В результате освоения дисциплины обучающийся должен **уметь**:
- использовать разные протоколы маршрутизации;
- настраивать базовые настройки сетевых устройств 2го уровня;
- уметь пользоваться научно технической литературой в области компьютерных сетей;
- настраивать параметры сетевых протоколов и служб для серверов, рабочих станций и активных сетевых устройств;
- определять техническое состояние локальной сети.

В результате освоения дисциплины обучающийся должен **знать**:
- основные принципы передачи информации по модели OSI;
- основу инфраструктуры компьютерных сетей и модульные зоны;
- требования к современным компьютерным сетям.
- основные виды сетевых архитектур и каналов передачи данных;
- основные характеристики построения различных видов сетей;
- основные виды и способы технической поддержки компьютерных сетей

При реализации содержания учебной дисциплины «Эксплуатация автоматизированных систем в защищенном исполнении» в пределах освоения ОПОП СПО на базе основного общего образования с получением среднего общего образования учебная нагрузка студентов составляет - 277 ч., из них аудиторная (обязательная) учебная нагрузка – 216 ч., включая лекции – 74 ч., практические занятия - 142 ч., консультации - 1 час; внеаудиторная самостоятельная работа студентов - 60 ч.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	*277*
Обязательная аудиторная учебная нагрузка (всего)	
в том числе:	
теоретическое обучение	*74*
лабораторные работы	-
практические занятия	*142*
контрольные работы	
консультации	*1*
Самостоятельная работа обучающегося (всего)	*60*
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	
Промежуточная аттестация в форме ***диф. зачета и экзамена***	

2.2. Тематический план и содержание дисциплины «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

Наименование разделов и тем	**Содержание учебного материала лабораторные и практические самостоятельная работа обучающихся,работа (проект)** ***(если предусмотрены)***	**Объем в часах**	***Формы и методы контроля и оценки результатов обучения***
6 семестр			
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		***120***	
Тема 1.1. Основы информационных систем как объекта защиты.	***Лекции***	***4***	
	1. Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная вязь. Требования к АИС: гибкость, надежность, эффективность, безопасность		
	2. Основные особенности современных проектов АИС. Электронный документооборот.		
	Семинарские занятия	***8***	Устный опрос, тестирование.
	1. Классификация автоматизированных информационных систем.		
	2. Классификация угроз		
	3. Нормативная база		
	4. Особенности объектов защиты		
	Практические занятия/Лабораторные занятия	***2***	
	Упражнения. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)		оценка умения, анализа и решения профессиональных задач.
Тема 1.2. Жизненный цикл автоматизированных систем	***Лекции***	4	
	1. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.		

	2.	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.		
	3.	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.		
	Семинарские занятия		6	Устный опрос, тестирование.
	1.	Жизненный цикл изделия. Этап эксплуатации, как основная цель		
	2.	Замысел, степень новизны, жизненный путь, жизненный цикл		
	3.	Потребность, цель и возможные последствия		
	Практические занятия/Лабораторные занятия		2	анализ, оценка, вопросы и диагностика фактического материала
	Лабораторная работа. 1. Разработка технического задания на проектирование автоматизированной системы			
	Самостоятельная работа обучающихся		10	коллоквиум
	1.	Разработка концепции защиты автоматизированной (информационной) системы		
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	***Лекции***		4	
	1.	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации.		
	2.	Понятие уязвимости угрозы. Классификация уязвимостей.		
	Семинарские занятия		8	Устный опрос, тестирование
	1.	Категорирование информационных ресурсов		
	2.	Анализ угроз безопасности информации		
	3.	Каналы утечки информации АИС		
	4.	Оценка угроз безопасности АИС		
	Практические занятия/Лабораторные занятия		2	оценка умения, анализа и решения профессиональных задач.
	Моделирование практической ситуации 1. Построение модели угроз			
	Самостоятельная работа обучающихся		10	тестирование

	1.	Анализ банка данных угроз безопасности информации		
Тема 1.4. Основные меры защиты информации в автоматизированных системах	***Лекции***		4	
	1.	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		
	2.	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним		
	Семинарские занятия		8	Устный опрос, тестирование.
	1.	Политика безопасности АИС		
	2.	Методы и средства защиты информации		
	Практические занятия/Лабораторные занятия		2	оценка умения, анализа и решения профессиональных задач.
	1.	Лабораторная работа		
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	***Лекции***		8	
	1.	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.		
	2.	Ограничение программной среды. Защита машинных носителей информации		
	3.	Регистрация событий безопасности		
	4.	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.		
	5.	Обнаружение (предотвращение) вторжений		
	6.	Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.		
	7.	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.		
	8.	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.		
	9.	Резервное копирование и восстановление данных.		

	10.	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.		
	Семинарские занятия		8	Устный опрос, самостоятельная работа
	1.	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении		
	2.	Защита входа в систему (идентификация и аутентификация пользователей)		
	3.	Разграничение доступа к устройствам. Управление доступом		
	4.	Использование принтеров для печати конфиденциальных документов. Контроль печати		
	Практические занятия/Лабораторные занятия		2	оценка умения, анализа и решения профессиональных задач.
	1.	Настройка системы для задач аудита		
	2.	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		
	3.	Настройка контроля целостности и замкнутой программной среды		
Тема 1.6. Защита информации в распределенных автоматизированных системах	***Лекции***		6	
	1.	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.		
	Семинарские занятия		6	Устный опрос, тестирование.
	1.	Планирование и реализация систем защиты		
	2.	Средства разграничения доступа		
	Практические занятия/Лабораторные занятия		2	оценка умения, анализа и решения профессиональных задач
	1.	Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации		
	Самостоятельная работа обучающихся		10	Коллоквиум, тестирование.
	1.	Изучение аналитических обзоров в области построения систем безопасности		
Тема 1.7.	***Лекции***		4	

Особенности разработки информационных систем персональных данных	1.	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.		
	Семинарские занятия		8	Устный опрос, тестирование, контрольная работа
	1.	Определения уровня защищенности информационных систем персональных данных и выбор мер по обеспечению безопасности персональных данных.		
	2.	Оценка угроз безопасности информационных систем персональных данных.		
	3.	Требования по защите персональных данных, в соответствии с уровнем защищенности		
	Практические занятия		2	оценка умения, анализа и решения профессиональных задач.
	Упражнения 1. Требования по защите сведений.			
Промежуточная аттестация в форме дифференцированного зачета				
7 семестр				
Раздел 2. Эксплуатация защищенных автоматизированных систем.			***79***	
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	***Лекции***		6	
	1.	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.		
	2.	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.		
	3.	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении		
	Семинарские занятия		10	Устный опрос, самостоятельная работа
	1.	Особенности эксплуатации автоматизированных систем в защищенном исполнении		
	2.	Особенности ведения эксплуатационной документации		
	Практические занятия/Лабораторные занятия		2	оценка умения, анализа и решения профессиональн
	У*пражнение* ***1.*** Методы мониторинга и аудита, выявления			

	угроз информационной безопасности автоматизированных систем			ых задач.
	Самостоятельная работа обучающихся		10	Тестирование, коллоквиум.
	1.	Анализ журнала аудита ОС на рабочем месте		
	2.	Построение сводной матрицы угроз автоматизированной (информационной) системы		
	3.	Анализ политик безопасности информационного объекта		
Тема 2.2. Администрирование автоматизированных систем	***Лекции***		6	
	1.	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.		
	Семинарские занятия		10	Тестирование, устный опрос.
	1.	Задачи и функции администрирования автоматизированных систем		
	2.	Автоматизация управления сетью. Организация администрирования автоматизированных систем.		
	3.	Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем.		
	4.	Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.		
	Практические занятия/Лабораторные занятия		2	анализ, оценка, вопросы и диагностика фактического материала
	Упражнения			
	Самостоятельная работа обучающихся		10	Коллоквиум
	1.	Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.		
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	***Лекции***		6	
	1.	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.		
	Семинарские занятия		10	Устный опрос, самостоятельная работа
	1.	Защита носителей информации резервное копирование и восстановлении данных.		

	2.	Сопровождение автоматизированных систем. Управление исками и инцидентами управления безопасностью.		
	3.	Обязанности администратора информационной безопасности автоматизированных систем.		
	Самостоятельная работа обучающихся		7	коллоквиум
	1.	Управление рисками и инцидентами управления безопасностью.		
Раздел 3. Защита от несанкционированного доступа к информации в автоматизированных системах			78	
Тема 3.1. Защита от несанкционированного доступа к информации	***Лекции***		6	
	1.	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.		
	2.	Классификация автоматизированных систем. Требования по защите информации от НСД для АС		
	3.	Требования защищенности СВТ от НСД к информации		
	4.	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ		
	Практические занятия/Лабораторные занятия		10	анализ, оценка, вопросы и диагностика фактического материала
	1.	Упражнения		
	Самостоятельная работа обучающихся		7	Тестирование
	1.	Изучение аналитических обзоров в области построения систем безопасности		
Тема 3.2. Система защиты информации от несанкционированного доступа	***Лекции***		6	
	1.	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.		
	2.	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов.		

		Управление грифами конфиденциальности.		
	3.	Обеспечение целостности информационной системы и информации		
	4.	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.		
		Семинарские занятия	10	Устный опрос, тестирование, контрольная работа
	1.	Установка и настройка СЗИ от НСД		
	2.	Защита входа в систему (идентификация и аутентификация пользователей)		
	3.	Разграничение доступа к устройствам		
	4.	Управление доступом		
	Практические занятия/Лабораторные занятия		4	анализ, оценка, вопросы и диагностика фактического материала
	1.	Использование принтеров для печати конфиденциальных документов. Контроль печати		
	2.	Настройка системы для задач аудита		
	3.	Настройка контроля целостности и замкнутой программной среды		
	4.	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		
		Самостоятельная работа обучающихся	7	тестирование
	1.	Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации		
Тема 3.3. Эксплуатация средств защиты информации в компьютерных сетях	***Лекции***		6	
	1.	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.		
	2.	Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации		
	3.	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении		
	4.	Настройка и устранение неисправности программно- аппаратных средств защиты информации в компьютерных сетях по заданным правилам		
		Семинарские занятия	10	Устный опрос,

	1.	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.		тестирование.
	2.	Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации		
	3.	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении		
	4.	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем		
Тема 3.4. Документация на защищаемую автоматизированную систему	***Лекции***		4	
	1.	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.		
	Семинарские занятия		8	Коллоквиум, тестирование.
	1.	Оформление основных эксплуатационных документов на автоматизированную систему.		
	2.	Особенности введения эксплуатационной документации		
Курсовая работа Примерная тематика курсовой работы Физическое кодирование с использованием манчестерского кода Логическое кодирование с использованием скремблирования Подключение клиента к беспроводной сети в инфраструктурном режиме Оценка беспроводной линии связи Проектирования беспроводной сети Сбор информации о клиентских устройствах Планирование производительности и зоны действия беспроводной сети Предпроектное обследование места установки беспроводной сети Обеспечение отказоустойчивости в беспроводных сетях Режимы работы и организация питания точек доступа Сегментация беспроводной сети Настройка QoS Постпроектное обследование и тестирование сети Создание ACL-списка Наблюдение за трафиком в сети VLAN Определение уязвимых мест сети Реализация функций обеспечения безопасности порта коммутатора Исследование трафика				

Создание структуры сети организации Определение технических требований Мониторинг производительности сети Создание диаграммы логической сети Подготовка к обследованию объекта Обследование зоны беспроводной связи Формулировка общих целей проекта Разработка требований к сети Анализ существующей сети Определение характеристик сетевых приложений Анализ сетевого трафика Определение приоритетности трафика Изучение качества обслуживания сети Исследование влияния видеотрафика на сеть Определение потоков трафика, построение диаграмм потоков трафика Применение проектных ограничений Определение проектных стратегий для достижения масштабируемости Определение стратегий повышения доступности Определение требований к обеспечению безопасности Разработка ACL-списков для реализации наборов правил межсетевого экрана Использование CIDR для обеспечения объединения маршрутов Определение схемы IP-адресации Определение количества IP-сетей Создание таблицы для выделения адресов Составление схемы сети Анализ плана тестирования и выполнение теста Создание плана тестирования для сети комплекса зданий Проектирование виртуальных частных сетей Безопасная передача данных в беспроводных сетях		
Промежуточная аттестация в форме экзамена		
Всего	***277***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия мультимедийной аудитории (с установленным проектором) и компьютерного кабинета.

Оборудование лаборатории и рабочих мест лаборатории:
- автоматизированное рабочее место преподавателя;
- автоматизированное рабочие места обучающихся (по количеству обучающихся в подгруппе);
- сетевое периферийное оборудование;
- периферийное оборудование для ввода и вывода информации;
- мультимедийное оборудование: проектор, экран;
- комплект учебно-наглядных пособий «Сети и система передачи информации».
- файловый сервер, локальная сеть;
- выход в глобальную сеть;
- комплект учебно-методической документации

Программное обеспечение:
Androind Studio, Brackets, Google Chrome, IIS Express, IntelliJ IDEA Community Edition, Java SE Development Kit, Microsoft Visual Studio Code, PascalABC.Net, PostgreSQL 12, Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016, Visio 2016, Adobe Photoshop

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 333 с. — URL : https://urait.ru/bcode/491456
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 351 с. — URL : https://urait.ru/bcode/491951
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с.— URL : https://urait.ru/bcode/476997
4. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2022. — 363 с.— URL : https://urait.ru/bcode/495353

Дополнительная литература:

1. Дибров М.В. Компьютерные сети и телекоммуникации. Маршрутизация в IP – сетях. В 2ч. Часть 1: учебник и практикум для СПО М.: Издательство Юрайт, 2020
2. Карпов В.Е., Коньков К.А. Основы операционных систем. Практикум Интуит НОУ, 2020
3. Коньков К.А., Карпов В.Е. Основы операционных систем. Интуит НОУ, 2016

4. Коньков К.А. Основы организации операционных систем Microsoft Windows Интуит НОУ, 2016
5. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации М.: Издательский центр «Академия», 2020.
6. Кузнецов С.Д. Введение в реляционные базы данных. Москва: Интуит НОУ, 2020.
7. Назаров С.В., Широков А.И. Современные операционные системы Интуит НОУ, 2019
8. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft Интуит НОУ, 2016

Интернет-ресурсы:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен **уметь:** – определять затраты при создании локальных сетей и применять типовые схемы при их проектировании; – определять техническое состояние локальной сети; – настраивать параметры сетевых протоколов и служб для серверов, рабочих станций и активных сетевых устройств; – использовать программно-аппаратные средства технического контроля	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; Экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач на создание локальной сети с определением затрат и применением соответствующих типовых схем проектирования; Экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач на определение технического состояния сети.

В результате освоения дисциплины обучающийся должен **знать:** - физические среды передачи данных; - общие принципы построения сетей; - основные виды сетевых архитектур и каналов передачи данных; - типы линий связи; - стандартизацию сетей; - основные характеристики построения различных видов сетей; - основные виды и способы технической поддержки компьютерных сетей; - стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование; - особенности протоколов канального уровня.	Интерпретация результатов устного опроса. Текущий контроль в форме тестирования. Текущий контроль усвоения материала в форме комбинированного опроса. Экспертная оценка результатов выполнения домашнего задания. Текущий контроль в форме комбинированного опроса. Экспертная оценка результатов выполнения домашнего задания.