АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«КУБАНСКИЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(АНПОО «КУБАНСКИЙ ИПО»)

ОТДЕЛЕНИЕ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
ОП.07 КОМПЬЮТЕРНЫЕ СЕТИ
по специальности
09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ
направленность программы: Веб-разработка

Краснодар, 2026

СОГЛАСОВАНО
Зам. директора по КОД и МР

_____ / Т.В. Першакова
28.05.2026 г.

УТВЕРЖДАЮ
Директор АНПОО «Кубанский ИПО»

_____ О.Л. Шутов
Приказ №38-О от 28.05.2026 г.

ОДОБРЕНО
Педагогическим советом
Протокол №6 от 28.05.2026 г

РАССМОТРЕНО
на заседании УМО
«Информационные системы и программирование»
Протокол № 5 от 15.05.2026г.
Председатель _____ / С.А. Пясецкий

Рабочая программа учебной дисциплины ОП.07 Компьютерные сети предназначена для реализации образовательной программы подготовки специалистов среднего звена.

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением (Приказ Министерства Просвещения Российской Федерации от 24 февраля 2025 г. № 138, зарегистрированного Министерством Юстиции России 31 марта 2025 г. № 81696) с учетом примерной образовательной программы, разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий, специальностей 09.00.00 Информатика и вычислительная техника, с учетом профессиональных стандартов: «Программист» (Приказ Министерства труда и социальной защиты РФ от 20 июля 2022 г. № 424н, зарегистрирован Министерством юстиции Российской Федерации от 22 августа 2022г. №69720); «Разработчик Web и мультимедийных приложений» (Приказ Министерства труда и социальной защиты РФ от 18 января 2017 г. № 44н, зарегистрирован Министерством юстиции Российской Федерации от 31 января 2017 г. № 45481) и компетенции «Веб- технологии».

Организация-разработчик: АНПОО «Кубанский ИПО»

Разработчик:
Пясецкий С.А., преподаватель АНПОО «Кубанский ИПО»

Рецензенты:
1. Варкентин В.Ф. – преподаватель, АНПОО «Кубанский ИПО»
Квалификация по диплому: преподаватель информатики
2. Маслиев Р.О, генеральный директор ООО «Старт Эксперт»

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.07 КОМПЬЮТЕРНЫЕ СЕТИ

1.1 Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.07 Компьютерные сети является обязательной частью общепрофессионального цикла образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций:

ОК.01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК.02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК.09. Пользоваться профессиональной документацией на государственном и иностранном языках;

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации;

ПК 3.3. Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием;

1.2 Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания.

Код ПК, ОК	Умения	Знания
ПК.1.5., ПК.3.3., ОК.01, ОК.04, ОК.09	− определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; − взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности; − понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; − анализировать требований безопасности информационных систем; − разрабатывать и реализовывать подсистемы безопасности информационных систем; − тестировать и проводить отладку подсистем безопасности информационных систем; − создавать и управлять защищенными соединениями с базой данных; − обеспечивать безопасность базы данных при использовании облачных сервисов; − *проектировать адресное пространство;* − *настраивать динамическую маршрутизацию OSPF с аутентификацией в многооблачной сети;* − *работать с IPv6;*	− актуальный профессиональный и социальный контекст, в котором приходится работать и жить; − структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; − принципы безопасности информационных систем; − современные методы и технологии в области безопасности информационных систем; − законодательных и нормативных актов в области безопасности информационных систем; − методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование; − методы обеспечения безопасности базы данных при использовании облачных сервисов, включая защиту от утечки данных и управление доступом к облачным ресурсам; − *методы проектирования адресного пространства;* − *принципы работы динамических протоколов маршрутизации в распределённых и облачных сетях;* − *структура и возможности протокола*

	− *автоматизировать сетевые задачи с помощью скриптов;* − *конфигурировать базовые протоколы ЦОД;* − *применять технологии SDN и NFV для виртуализации сетевых функций;* − *обеспечивать безопасность беспроводных сетей;* − *проводить тестирование подсистем безопасности;* − *управлять защищенными соединениями с базой данных;* − *обеспечивать безопасность баз данных в облаке;* − *защищать облачные API;* − *применять методы CASB и DLP для мониторинга облачных сервисов и предотвращения утечек данных;* − *анализировать сетевой трафик для выявления инцидентов;* − *разрабатывать комплексные подсистемы безопасности на основе технического задания (ТЗ);* − *представлять и защищать проектные решения на русском и иностранном (английском) языке с использованием профессиональной терминологии.*	*IPv6;* − *основы сетевого программирования и автоматизации;* − *архитектура и принципы SDN (программируемые сети) и NFV (виртуализация сетевых функций);* − *современные стандарты безопасности беспроводных сетей;* − *методики тестирования и отладки подсистем безопасности;* − *способы создания и управления защищенными соединениями с БД;* − *модели обеспечения безопасности баз данных в облачных средах;* − *принципы защиты облачных API;* − *назначение и функции CASB (Cloud Access Security Broker) и DLP (Data Loss Prevention) в контексте защиты облачных сервисов и предотвращения утечек;* − *методы анализа сетевого трафика для расследования инцидентов;* − *этапы разработки подсистемы безопасности по техническому заданию;* − *профессиональная терминология на иностранном (английском) языке в области компьютерных сетей и безопасности.*

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
ОБЪЕМ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	**80**
в том числе вариативная часть	*40*
- теоретическое обучение	**40**
- практические занятия	**40**
в т.ч. в форме практической подготовки	40
- промежуточная аттестация (дифференцированный зачет)	**2**

Тематический план учебной дисциплины

Наименование разделов и тем	Количество аудиторных часов				
	Всего	**в т.ч. в форме практической подготовки**	**самост. работа**	**теоретич. обучение**	**практич. занятия**
Раздел 1. Компьютерные сети	**78**	**40**	**-**	**40**	**38**
Тема 1.1 Основы компьютерных сетей и сетевые модели	8	**4**	**-**	4	4
Тема 1.2 Адресация, протоколы и базовая настройка сетей	22	10	-	12	10
Тема 1.3 Среды передачи данных и оборудование	16	8	-	8	8
Тема 1.4 Безопасность компьютерных сетей	24	12	-	12	12
Тема 1.5 Сетевые архитектуры и комплексные проекты	8	4	-	4	4
Дифференцированный зачет	**2**	**2**	**-**	**-**	**2**
ВСЕГО	**80**	**40**	**-**	**40**	**40**

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Компьютерные сети		**78**	
Тема 1.1 Основы компьютерных сетей и сетевые модели	**Содержание учебного материала**	**8**	ОК.01, ОК.02, ОК.09 ПК1.5
	1 **Понятие компьютерной сети. Компоненты и классификация** Определение компьютерной сети. Основные компоненты: узлы (компьютеры, серверы, принтеры), каналы связи (проводные и беспроводные), сетевое оборудование, протоколы. Актуальный профессиональный контекст: применение сетей (офис, ЦОД, облака, промышленность, умный дом). Классификация сетей: LAN (локальные), MAN (городские), WAN (глобальные); клиент-серверные и одноранговые; проводные и беспроводные. Примеры задач: выбрать тип сети для малого офиса или распределенной компании. *Сравнение «традиционных» сетей и сетей следующего поколения. Краткое введение в понятие «цифровая трансформация»: влияние сетей на бизнес-процессы (облачные сервисы, удалённая работа, IoT). Обсуждение профессионального и социального контекста: анализ востребованности специалистов по сетям и безопасности на рынке труда. Знакомство с профессиональной документацией на английском языке: чтение фрагмента RFC (например, RFC 1122 «Requirements for Internet Hosts») с выделением ключевых терминов (host, router, protocol stack)*	2	
	2 **Модели OSI и TCP/IP. Инкапсуляция протоколов** Понятие сетевой модели. Зачем нужны уровни. Модель OSI: 7 уровней (от физического до прикладного), функции каждого уровня. Взаимодействие через интерфейсы. Модель TCP/IP: 4 уровня (сетевых интерфейсов, интернет, транспортный, прикладной). Соответствие уровням OSI. Инкапсуляция данных: как пакет «обрастает» заголовками. План решения задач: как локализовать неисправность по уровню модели. *Сравнение модели OSI и TCP/IP с практической точки зрения. Расширенный пример инкапсуляции с анализом реального пакета в Wireshake. Работа с профессиональной документацией на иностранном языке: изучение фрагмента RFC 791 (IP) и RFC 793 (TCP)*	2	
	в том числе, практических занятий	**4**	
	***ПЗ №1.** Расчет IP-адреса, маски подсети, номера сети, широковещательного адреса, количества хостов	2	
	***ПЗ №2.** Команды ping, traceroute (tracert), netstat. Анализ маршрута, времени ответа, открытых портов	2	
Тема 1.2 Адресация, протоколы и базовая настройка сетей	**Содержание учебного материала**	**22**	ОК.01, ОК.02, ПК.3.3
	3 **IPv4-адресация: классы, маски, CIDR, шлюзы** Структура IPv4-адреса (32 бита, десятичный вид). Классы A, B, C, D, E. Понятие сетевой и хостовой части. Маска подсети (префикс). CIDR (бесклассовая адресация). Шлюз по умолчанию (default gateway). Примеры расчета сетей разного размера.	2	

	4	***IPv6: адресация и автоконфигурация*** *Формат IPv6 (128 бит, шестнадцатеричная запись). Типы адресов: unicast, anycast, multicast. Link-local, unique local, глобальные адреса. SLAAC (Stateless Address Autoconfiguration), EUI-64. Настройка IPv6 на маршрутизаторе.*	*2*	
	5	**Транспортные и прикладные протоколы. Порты** TCP: установка соединения (3-way handshake), надежность, подтверждения, сегментация. UDP: без установки соединения, дейтаграммы, низкая задержка. Номера портов (well-known, зарегистрированные, динамические). Примеры: TCP для HTTP/HTTPS, UDP для DNS, VoIP, игр. Взаимодействие с верхними уровнями. DNS: имена в IP, иерархия, типы записей. DHCP: автоматическая выдача IP, аренда, опции (шлюз, DNS). HTTP/HTTPS: методы (GET, POST), коды ответа, безопасность (TLS). FTP: активный/пассивный режимы, команды. SMTP, POP3, IMAP для почты. Анализ информации	2	
	6	**Маршрутизация и VLAN. Статика и динамика** Таблица маршрутизации. Статическая маршрутизация (ip route). Динамические протоколы: RIP (дистанционно-векторный), OSPF (состояние каналов). VLAN: зачем делить сеть, теги 802.1Q, транки, access-порты. Безопасность: изоляция трафика. *IPv6 в контексте маршрутизации. Как статическая маршрутизация выглядит в IPv6 (ipv6 route). Динамическая маршрутизация для IPv6: OSPFv3 (отличия от OSPFv2).*	2	
	7	***Современные протоколы маршрутизации для ЦОД: BGP, EVPN*** *BGP (Border Gateway Protocol) — iBGP/eBGP, атрибуты, сообщества. EVPN (Ethernet VPN) для мультитенантных сетей. Сценарии использования в дата-центрах и облаках.*	*2*	
	8	***Основы сетевого программирования (Python сокеты) для автоматизации*** *Библиотека socket. Создание TCP/UDP клиента и сервера. Автоматизация ping, telnet/SSH к оборудованию (netmiko, paramiko). Скрипт для сборки таблицы ARP со всех маршрутизаторов.*	*2*	
	в том числе, практических занятий		**10**	
	****ПЗ №3.*** *Расширенное проектирование адресации: VLSM и суммирование маршрутов*		*2*	
	***ПЗ №4.** Настройка статической маршрутизации		2	
	***ПЗ №5.** Обмен данными через TCP и UDP. Настройка DHCP и DNS-серверов		2	
	***ПЗ №6.** Настройка VLAN, удаленный доступ (SSH, RDP)		2	
	****ПЗ №7.*** *Динамическая маршрутизация OSPF с аутентификацией*		*2*	
Тема 1.3 Среды передачи данных и оборудование	**Содержание учебного материала**		**16**	ОК.02, ОК.09, ПК.1.5, ПК.3.3
	9	**Физические среды передачи. Методы доступа к среде** Типы кабелей: витая пара (UTP, FTP, категории 5e/6/7/8), коаксиал, оптоволокно (одномодовое/многомодовое). Характеристики: полоса пропускания, затухание, помехозащищенность, дальность. Беспроводные: Wi-Fi (802.11a/b/g/n/ac/ax/be), частоты 2.4/5/6 ГГц, Bluetooth, Zigbee. Проблема множественного доступа. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – для Ethernet. Коллизии, jam-сигнал, бэкофф. CSMA/CA (Collision Avoidance) – для Wi-Fi. RTS/CTS, окна ожидания. Сравнение эффективности.	2	
	10	**Сетевое оборудование: коммутаторы, маршрутизаторы, шлюзы, адаптеры** Коммутаторы (L2): таблица MAC-адресов, фильтрация, широковещательные домены. Маршрутизаторы	2	

		(L3): маршрутизация, NAT, ACL. Мосты, шлюзы (в т.ч. шлюзы приложений). Сетевые адаптеры: PCIe, USB, драйверы, аппаратные очереди. *SDN и NFV — виртуализация сетевых функций. Современные технологии беспроводной безопасности. Автоматизация и программируемость оборудования*		
	11	***Технологии SDN и NFV*** *SDN (Software-Defined Networking): разделение плоскости управления и данных, контроллер (OpenFlow). NFV (Network Functions Virtualization): виртуализация маршрутизаторов, файрволов. Примеры: Mininet, Open vSwitch.*	*2*	
	12	***Беспроводная безопасность: WPA3, 802.1X, RADIUS*** *Уязвимости WPA2 (KRACK). WPA3: SAE (Simultaneous Authentication of Equals), OWE. 802.1X (EAP) – порт-ориентированная аутентификация. RADIUS-сервер (FreeRADIUS). Интеграция с Active Directory.*	*2*	
	в том числе, практических занятий		**8**	
	ПЗ №8. Обжим кабеля и тестирование линий		2	
	ПЗ №9. Базовая настройка маршрутизатора и сетевых адаптеров		2	
	ПЗ №10. Имитация CSMA/CD и CSMA/CA. Межсетевой экран (ACL)		2	
	ПЗ №11. *Настройка Wi-Fi безопасности: WPA3-Enterprise и RADIUS*		*2*	
Тема 1.4 Безопасность компьютерных сетей	**Содержание учебного материала**		**24**	ПК.1.5, ПК.3.3, ОК.01, ОК.09
	13	**Основы безопасности сетей. Угрозы и принципы** Основные угрозы: перехват (sniffing), модификация, подмена, DoS/DDoS, MITM. Принципы безопасности ИС: конфиденциальность (шифрование), целостность (хеши), доступность (отказоустойчивость).	2	
	14	**Законодательная база РФ в области безопасности ИС** ФЗ-149 «Об информации, информационных технологиях и о защите информации», ФЗ-152 «О персональных данных», Приказы ФСТЭК (например, о СЗИ). Ответственность за утечки. Требования к защите БД. Работа с документацией на русском языке. *Анализ требований безопасности информационных систем. Облачная безопасность и законодательство РФ*	2	
	15	**Методы защиты, управление доступом к БД. Разработка подсистем по ТЗ** VPN-туннели: IPsec (ESP/AH, IKE), OpenVPN, WireGuard. SSL/TLS: сертификаты, handshake, шифрование трафика. Управление доступом к БД: роли, привилегии, аудит. Облачные ресурсы: IAM, Bucket policies. Этапы разработки подсистемы: анализ угроз, выбор мер, реализация, тестирование. Отладка безопасности: логи, мониторинг, реагирование. *Защита соединений с БД (VPN-туннель к БД как дополнительный слой защиты). Использование KMS (Key Management Service) для шифрования данных в облачной БД (AWS KMS, Yandex KMS, Azure Key Vault).*	2	
	16	***Методы тестирования и отладки подсистем безопасности*** *Виды тестирования: сканирование уязвимостей (nmap, OpenVAS), пентест (методология OWASP). Отладка политик безопасности: анализ логов, корректировка ACL/правил. Инструменты: Wireshark, tcpdump, fail2ban, Snort (базово).*	*2*	
	17	***Управление защищенными соединениями с БД: VPN, SSL, прокси*** *SSL-шифрование для PostgreSQL/MySQL (require, verify-full). VPN-туннель к БД в облаке или ЦОД. Балансировка и отказоустойчивость соединений (PgBouncer с SSL).*	*2*	

	18	***Облачная безопасность: CASB, DLP, защита API*** *CASB (Cloud Access Security Broker) для мониторинга облачных сервисов. DLP (Data Loss Prevention) – защита от утечек. Безопасность REST API: аутентификация (JWT, OAuth2), rate limiting, валидация.*	*2*	
	в том числе, практических занятий		**12**	
	ПЗ №12. Разработка политики сетевой безопасности		2	
	ПЗ №13. Сбор и анализ сетевого трафика		2	
	ПЗ №14. *Настройка HTTPS на веб-сервере и VPN-туннеля*		*2*	
	ПЗ №15. *Разработка подсистемы безопасности по ТЗ*		2	
	ПЗ №16. *Тестирование подсистемы безопасности (nmap, OpenVAS, отладка)*		2	
	ПЗ №17. *Обеспечение безопасности БД в облаке*		2	
Тема 1.5 Сетевые архитектуры и комплексные проекты	**Содержание учебного материала**		**8**	ПК.1.5, ПК.3.3, ОК.01, ОК.09
	19	**Принципы построения КС. Иерархические модели. WAN** Иерархическая модель: ядро (Core), распределение (Distribution), доступ (Access). Технологии глобальных сетей: MPLS, SD-WAN, L2VPN/L3VPN. Отказоустойчивость: STP, LACP, VRRP. *Сравнение MPLS и SD-WAN с точки зрения безопасности (шифрование трафика по умолчанию в SD-WAN, изоляция VRF в MPLS).*	2	
	20	**Облачные сервисы и безопасность баз данных в облаке** Облачные модели: IaaS, PaaS, SaaS. Безопасность БД в облаке: защита от утечек (шифрование, DLP), управление доступом (IAM, RBAC), аудит. Инструменты: AWS RDS, Azure SQL, облачные ключи шифрования (KMS). *Модели ответственности (Shared Responsibility Model). Краткий обзор облачных платформ, доступных в РФ: Yandex Cloud (Managed Service for PostgreSQL), VK Cloud, SberCloud, Selectel.*	2	
	в том числе, практических занятий		**4**	
	ПЗ №18. Построение компьютерной сети (сборка проекта)		2	
	ПЗ №19. *Построение корпоративной сети с защищенным сегментом БД через VPN-туннель*		2	
Дифференцированный зачет (ПЗ №20)			**2**	
ВСЕГО:			**80**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория «Компьютерных сетей и основ информационной безопасности»

оснащена оборудованием:

− рабочее место педагога (преподавательский стол (1 шт.), стул (1 шт.))
− рабочие места обучающихся (парты ученические (13 шт.), стулья ученические (25 шт.))
− доска учебная (меловая трех-секционная) (1 шт.)
− книжный шкаф – 1 шт.;
− учебно-методическая литература по дисциплине;
− комплект учебно-наглядных пособий;

техническими средствами обучения:

− персональный компьютер, подключение к сети Интернет с модулем контентной фильтрации Traffic Inspector, NetPolice и YandexDNS, возможность трансляции на экран аудио и видео информации (1 шт.)
− программное обеспечение на ПК – Microsoft Windows 10 или аналог, Microsoft Office (Word, Excel, PowerPoint) или аналог, 7Zip, 24PDF, Яндекс Браузер (1 шт.)
− программное обеспечение Android Studio, Visual Studio, Visual Studio Code или налоги
− монитор (1 шт.)
− клавиатура (1 шт.)
− мышь (1 шт.)
− телевизор (1 шт.)
− кабель для подключения HDMI (1 шт.)

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд института имеет печатные и электронные образовательные и информационные ресурсы, в том числе рекомендованные ФУМО, для использования в образовательном процессе. Список дополнен новыми изданиями.

3.2.1 Основные источники

1. Акмаров, П. Б. Компьютерные сети. Лабораторный практикум / П. Б. Акмаров. — Санкт-Петербург : Лань, 2024. — 120 с. — ISBN 978-5-507-48068-5. — Текст : электронный
2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 423 с. — (Профессиональное образование). — ISBN 978-5-534-16551-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589270
3. Компьютерные и телекоммуникационные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 96 с. — (Профессиональное образование). — ISBN 978-5-534-21456-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590201
4. Компьютерные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590199
5. Кузин, А. В. Компьютерные сети : учебное пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2025. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. - Текст: электронный.

6. Рабчевский, А. Н. Компьютерные сети и системы связи. Вводный курс : учебник для среднего профессионального образования / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2026. — 185 с. — (Профессиональное образование). — ISBN 978-5-534-22195-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/600888

7. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 464 с. — (Профессиональное образование). — ISBN 978-5-534-17310-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587334

3.2.2 Дополнительные источники

8. Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — ISBN 978-5-9997-0805-2. — Текст : электронный

9. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебник для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2025. — 167 с. — (Профессиональное образование). — ISBN 978-5-534-17558-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566086

10. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для среднего профессионального образования / Л. А. Станкевич. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 478 с. — (Профессиональное образование). — ISBN 978-5-534-20364-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587749

11. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. - Москва ; Вологда : Инфра-Инженерия, 2022. - 460 с. - ISBN 978-5-9729-0962-9. - Текст : электронный.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
Уметь: − определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; − взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности; − понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; − анализировать требований безопасности информационных систем; − разрабатывать и реализовывать подсистемы безопасности информационных систем; − тестировать и проводить отладку подсистем безопасности информационных систем; − создавать и управлять защищенными соединениями с базой данных; − обеспечивать безопасность базы данных при использовании облачных сервисов; − *проектировать адресное пространство;* − *настраивать динамическую маршрутизацию OSPF с аутентификацией в многооблачной сети;* − *работать с IPv6;* − *автоматизировать сетевые задачи с помощью скриптов;* − *конфигурировать базовые протоколы ЦОД;* − *применять технологии SDN и NFV для виртуализации сетевых функций;* − *обеспечивать безопасность беспроводных сетей;* − *проводить тестирование подсистем безопасности;* − *управлять защищенными соединениями с базой данных;* − *обеспечивать безопасность баз данных в облаке;* − *защищать облачные API;* − *применять методы CASB и DLP для мониторинга облачных сервисов и предотвращения утечек данных;*	Умеет распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; организовывать и конфигурировать компьютерные сети; строить и анализировать модели компьютерных сетей; работать с протоколами разных уровней; устанавливать и настраивать параметры протоколов *проектировать адресное пространство с использованием VLSM и суммирования маршрутов;*	**Текущий контроль:** Компьютерное тестирование по основным разделам программы. Решение задач по основным разделам программы **Промежуточная аттестация:** дифференцированный зачет

− *анализировать сетевой трафик для выявления инцидентов;* − *разрабатывать комплексные подсистемы безопасности на основе технического задания (ТЗ);* *представлять и защищать проектные решения на русском и иностранном (английском) языке с использованием профессиональной терминологии.*	*настраивать динамическую маршрутизацию OSPF с аутентификацией в многооблачной сети;* *работать с IPv6: назначать адреса и настраивать автоконфигурацию (SLAAC);* *автоматизировать сетевые задачи с помощью скриптов на Python;* *конфигурировать базовые протоколы BGP и EVPN для мультитенантных сред;* *применять технологии SDN и NFV для виртуализации сетевых функций;* *обеспечивать безопасность беспроводных сетей с использованием WPA3-Enterprise и RADIUS;* *проводить тестирование подсистем безопасности (сканирование уязвимостей, отладка политик);* *управлять защищенными соединениями с базой данных (SSL, VPN-туннели);* *обеспечивать безопасность баз данных в облаке (IAM, Security Groups, шифрование KMS, аудит);* *защищать облачные API с использованием JWT, OAuth2 и rate limiting;* *применять методы CASB и DLP для мониторинга облачных сервисов;* *анализировать сетевой трафик для выявления инцидентов (сканирование, ARP-spoofing);* *разрабатывать подсистемы безопасности по техническому заданию (полный цикл: анализ угроз → тестирование);* *представлять и защищать проектные решения на русском и иностранном (английском) языке;* *анализировать профессиональный и социальный контекст для обоснования выбора сетевых решений;* *извлекать ключевую информацию из RFC и стандартов на английском языке;*	
Знать: − актуальный профессиональный и социальный контекст, в котором приходится работать и жить; − структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; − принципы безопасности информационных систем; − современные методы и технологии в области безопасности	Знает актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач;	**Текущий контроль:** Оценка результатов выполнения практической работы Экспертное наблюдение за ходом выполнения практической работы (деятельностью студента) Оценка выполнения

информационных систем; − законодательных и нормативных актов в области безопасности информационных систем; − методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование; − методы обеспечения безопасности базы данных при использовании облачных сервисов, включая защиту от утечки данных и управление доступом к облачным ресурсам; − *методы проектирования адресного пространства;* − *принципы работы динамических протоколов маршрутизации в распределённых и облачных сетях;* − *структура и возможности протокола IPv6;* − *основы сетевого программирования и автоматизации;* − *архитектура и принципы SDN (программируемые сети) и NFV (виртуализация сетевых функций);* − *современные стандарты безопасности беспроводных сетей;* − *методики тестирования и отладки подсистем безопасности;* − *способы создания и управления защищенными соединениями с БД;* − *модели обеспечения безопасности баз данных в облачных средах;* − *принципы защиты облачных API;* − *назначение и функции CASB (Cloud Access Security Broker) и DLP (Data Loss Prevention) в контексте защиты облачных сервисов и предотвращения утечек;* − *методы анализа сетевого трафика для расследования инцидентов;* − *этапы разработки подсистемы безопасности по техническому заданию;* *профессиональная терминология на иностранном (английском) языке в области компьютерных сетей и безопасности.*	порядок оценки результатов решения задач профессиональной деятельности номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств особенности социального и культурного контекста; правила оформления документов и построения устных сообщений правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование сетевые протоколы; технологии локальных сетей; общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям *принципы VLSM (маски переменной длины), CIDR (бесклассовую адресацию), методы суммирования маршрутов (route aggregation) и правила составления адресного плана для сетей с распределённой филиальной структурой.* *отличия дистанционно-векторных протоколов (RIP) от протоколов состояния каналов (OSPF), а также особенности применения BGP и EVPN в мультитенантных средах и облачных ЦОД.* *формат 128-битного IPv6-адреса (шестнадцатеричная запись, сжатие нулей), типы адресов (link-local, unique local, глобальные, мультикаст) и механизмы автоконфигурации (SLAAC, EUI-64).*	практического задания (работы) **Промежуточная аттестация:** дифференцированный зачет

	базовые возможности библиотеки socket (TCP/UDP), принципы работы netmiko/paramiko для управления оборудованием, а также возможности Ansible для массовой настройки коммутаторов и маршрутизаторов. *разделение плоскости управления и данных в SDN, роль контроллера (OpenFlow), концепцию виртуализации сетевых функций (NFV) и примеры (vRouter, vSwitch, виртуальные файрволы).* *отличия WPA2 от WPA3, принципы работы SAE (Simultaneous Authentication of Equals), технологию 802.1X (порт-ориентированная аутентификация) и роль RADIUS-сервера в корпоративных Wi-Fi сетях.* *базовые методы сканирования портов (nmap), поиска уязвимостей (OpenVAS), анализа отчётов, а также подходы к отладке политик доступа (ACL, правила файрвола) по логам.* *методы SSL/TLS-шифрования соединений с базами данных (PostgreSQL, MySQL) с проверкой подлинности сервера (require, verify-full), а также организацию доступа к БД через VPN-туннели (OpenVPN, IPsec, WireGuard).* *модель разделения ответственности (Shared Responsibility Model), принципы IAM (пользователи, роли, политики), использование Security Groups (групп безопасности), шифрование дисков и бэкапов через KMS, а также аудит доступа в облачных БД (AWS RDS, Yandex Cloud, Azure SQL).* *механизмы аутентификации и авторизации (JWT, OAuth2), методы ограничения частоты запросов (rate limiting), важность валидации входных данных и базовые практики безопасности REST API.* *что такое CASB (посредник между пользователями и облачными сервисами для контроля доступа) и DLP (системы предотвращения утечек), а также умеет объяснить их роль на примере обнаружения передачи паспортных данных через облачную почту или хранилище.* *возможности Wireshark (фильтры по IP, портам, протоколам), признаки порт-сканирования и ARP-spoofing в дампе трафика, а также методы восстановления сессий (Follow TCP Stream).*	

	полный жизненный цикл: анализ угроз и моделирование нарушителя, выбор организационных и технических мер защиты, реализация (настройка СЗИ, разработка модулей), функциональное тестирование и тестирование на проникновение, эксплуатация и отладка по результатам мониторинга. корректный перевод и значение ключевых терминов на английском языке, таких как: IPsec tunnel, database encryption, access control list (ACL), vulnerability scan, cloud IAM, security group, encryption at rest / in transit, key management service (KMS), audit logs, certificate chain, perfect forward secrecy (PFS), least privilege, incident response plan, и умеет использовать их при чтении RFC, документации облачных провайдеров и при защите проектов.	