Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 06.11.2026 16:26:52
Уникальный программный ключ:
637517d24e103c3db032acf37e839d98ec1c5bb2f5eb89c29abfcd7f43985447

Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
(МЕЖДУНАРОДНЫЙ ДИПЛОМАТИЧЕСКИЙ КОЛЛЕДЖ)

УТВЕРЖДАЮ
Директор Международного
дипломатического колледжа
_____ Н.И. Платонова
«16» февраля 2026г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

ОП.07 Компьютерные сети

Специальность
09.02.11 Разработка и управление программным обеспечением

Квалификация выпускника:
Программист

на базе основного общего образования

Форма обучения: очная

Москва

Фонд оценочных средств для дисциплины «ОП.07 Компьютерные сети». Специальность 09.02.11 Разработка и управление программным обеспечением /– М.: ИМПЭ им. А. С. Грибоедова.

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины.

Организация-разработчик:	Образовательное частное учреждение высшего образования «Московский университет имени А. С. Грибоедова»

Директор Международного
дипломатического колледжа_____/Н.И. Платонова

1. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Настоящий Фонд оценочных средств (ФОС) по дисциплине «ОП.07 Компьютерные сети» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «ОП.07 Компьютерные сети». На данный ФОС распространяются все реквизиты утверждения, представленные в РПД по данной дисциплине.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

Для определения качества освоения обучающимися учебного материала по дисциплине используются следующие оценочные средства:

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Тестирование	Вид контроля, позволяющий оценить изученный теоретический материал.	Вопросы для проведения тестирования
2	Практические задания	Вид контроля, позволяющий оценить умение обучающегося применять осваиваемую компетенцию в практических ситуациях и при решении производственных задач	Задания к практическому занятию
3	Контрольная работа	Вид контроля, позволяющий определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций	Задания контрольной работы
4	Самостоятельная работа	Вид контроля, позволяющий оценить проработку теоретического материала, изучение рекомендуемой литературы, выполнение практико-ориентированных заданий (заполнение таблиц, проведение сравнительного анализа, составление схем и др.), решение практических задач, создание презентаций, написание рефератов, подборку нормативного и иного материала и выполнение других заданий	Задания самостоятельной работы
5.	Зачет/Зачет с оценкой/Экзамен	Вид контроля, позволяющий выявить степень овладения знаниями, умениями и навыками, необходимыми для дальнейшего освоения образовательной программы подготовки	Вопросы для подготовки к зачету/зачету с оценкой/экзамену

3.ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Темы для подготовки к промежуточной аттестации

1. Модели сетевого взаимодействия OSI и TCP/IP: назначение, уровни и их сравнительный анализ.
2. Принципы пакетной коммутации и отличие от коммутации каналов. Понятия кадра, пакета, сегмента/датаграммы.
3. Физический и канальный уровни: основные среды передачи данных, понятие MAC-адреса и протокол ARP.
4. Сетевой уровень: функции и задачи. Принципы маршрутизации (статическая, динамическая).
5. Транспортный уровень: сравнительный анализ протоколов TCP и UDP, их характеристики и области применения.
6. Прикладной уровень: назначение и примеры ключевых протоколов (HTTP, DNS, SMTP, FTP). 7. IP-адресация IPv4: структура адреса, классы сетей, маска подсети.
8. Бесклассовая адресация (CIDR): принцип, расчет сетевого адреса, широковещательного адреса и диапазона хостов.
9. Специальные IPv4-адреса (private, loopback, APIPA) и их назначение.
10. IPv6: преимущества перед IPv4, структура адреса, типы адресов (unicast, multicast, anycast).
11. Протокол DNS: назначение, принцип работы (итеративные и рекурсивные запросы), типы записей (A, AAAA, CNAME, MX).
12. Протокол DHCP: назначение, принцип работы (DORA-процесс), понятие аренды адреса.
13. Протокол HTTP/1.1 и HTTP/2: методы запросов (GET, POST), структура сообщения, основные заголовки.
14. Протокол HTTPS: принцип работы TLS/SSL, назначение сертификатов.
15. Технология NAT (Network Address Translation): назначение, типы (Static, Dynamic, PAT/NAPT).
16. Сетевые устройства: концентратор (hub), коммутатор (switch), маршрутизатор (router). Принцип работы и уровень модели OSI.
17. Виртуальные локальные сети (VLAN): назначение, принцип работы (tagging по стандарту IEEE 802.1Q).
18. Основы сетевой безопасности: понятия брандмауэра (firewall), DMZ, типы сетевых атак (DoS, MITM, сканирование портов).
19. Сокеты (sockets) как основной API для сетевого программирования. Различия между потоковыми (TCP) и датаграммными (UDP) сокетами.
20. Этапы установления TCP-соединения (three-way handshake) и его завершения.
21. Инструменты командной строки для диагностики сетей в ОС Windows (ipconfig, ping, tracert, netstat) и Linux (ifconfig/ip, ping, traceroute, ss).
22. Анализ сетевого трафика: назначение и базовые принципы работы с анализатором трафика (например, Wireshark).
23. Беспроводные сети Wi-Fi: основные стандарты (IEEE 802.11 a/b/g/n/ac/ax), понятия SSID, методы аутентификации и шифрования (WPA2, WPA3).

24. Основы облачных сетей: понятия VPC (Virtual Private Cloud), подсетей, интернетшлюза.
25. Контейнеризация и сети: типы сетей Docker (bridge, host, none), принцип связи контейнеров.
26. Веб-сокеты (WebSockets): назначение, отличия от HTTP, область применения (realtime приложения).
27. Принципы REST API: ключевые ограничения архитектуры, использование методов HTTP, форматы данных (JSON/XML).
28. Протоколы электронной почты: SMTP для отправки, POP3 и IMAP для получения.
29. Системы контроля версий в сетевом контексте: работа с удаленными репозиториями (Git), протоколы доступа (SSH, HTTPS).
30. Принципы балансировки сетевой нагрузки (Load Balancing): цели и базовые алгоритмы (round-robin, наименьших соединений).
31. Сетевые файловые системы и протоколы: назначение и принципы работы NFS и SMB/CIFS.
32. Протоколы удаленного доступа: Telnet (небезопасный) и SSH (безопасный). Принцип аутентификации по ключу.
33. Технология виртуальных частных сетей (VPN): назначение, типы (например, Siteto-Site, Remote Access).
34. Системы доменных имен (DNS): кеширующие DNS-серверы, корневые серверы, проблемы безопасности (DNS spoofing).
35. Сетевые атаки на уровне приложений: SQL-инъекции, XSS, CSRF — общий принцип и меры противодействия для разработчика.
36. Мониторинг сетей: ключевые метрики (загрузка канала, потери пакетов, задержка), базовые принципы работы систем мониторинга.
37. Автоматизация сетевых задач: использование скриптов (bash/PowerShell, Python) для конфигурации и диагностики.
38. Принципы QoS (Quality of Service) в сетях: назначение, основные механизмы (классификация, маркировка, очереди).
39. Сетевые модели клиент-сервер и P2P (peer-to-peer): сравнительный анализ.
40. Протокол ICMP: назначение, использование в утилитах ping и traceroute.
41. Сетевые порты: понятие, диапазоны (well-known, registered, dynamic), связь портов с сокетами.
42. Документирование сетевой архитектуры проекта: диаграммы развертывания, описание используемых портов и протоколов.
43. Проблемы сетевой связности: типичный алгоритм диагностики (от локальных настроек до удаленного хоста).
44. Протоколы динамической маршрутизации: общее представление о OSPF и BGP (назначение, сфера применения).
45. Принципы работы CDN (Content Delivery Network): цели и преимущества использования.
46. Сетевое оборудование для разработчика: стенды для тестирования (виртуальные машины, эмуляторы сетей).
47. Форматы данных для сетевого обмена: JSON, XML. Их сравнительный анализ.

48. Основы отказоустойчивости сетевых приложений: стратегии повторных попыток (retry), использование нескольких endpoint'ов.
49. Сетевые требования для развертывания веб-приложения: открытие портов, настройка брандмауэра, привязка доменного имени.
50. Тенденции в развитии компьютерных сетей: программно-конфигурируемые сети (SDN), принципы работы 5G, интернет вещей (IoT) с точки зрения разработчика ПО.

Темы для самостоятельной работы обучающихся

1. Модели OSI и TCP/IP: сравнительный анализ, назначение каждого уровня и примеры протоколов.
2. Принципы пакетной коммутации: анализ преимуществ и недостатков по сравнению с коммутацией каналов.
3. IP-адресация IPv4: практическое освоение расчета подсетей, сетевых адресов, широковещательных адресов и диапазонов хостов с использованием CIDR.
4. Протокол IPv6: изучение структуры адреса, типов адресов (unicast, multicast, anycast) и методов перехода с IPv4 (туннелирование, dual-stack).
5. Анализ сетевого трафика: самостоятельное изучение основ работы с анализатором трафика (Wireshark) для захвата и фильтрации пакетов.
6. Сравнительный анализ транспортных протоколов TCP и UDP: сферы применения, механизмы надежности и управления потоком в TCP.
7. Этапы установления и завершения TCP-сессии: детальный разбор процесса threeway handshake и four-way handshake termination.
8. Система доменных имен (DNS): углубленное изучение типов DNS-записей (A, AAAA, CNAME, MX, TXT, SRV) и принципов работы кеширующих DNSсерверов.
9. Диагностика сетевых проблем: составление универсального алгоритма действий с использованием утилит ping, traceroute, netstat/ss, nslookup/dig.
10. Принципы работы протокола DHCP: детальный разбор процесса DORA (Discover, Offer, Request, Acknowledge) и понятия аренды адреса.
11. Технология NAT (трансляция сетевых адресов): изучение типов (Static NAT, Dynamic NAT, PAT/NAPT) и их практического применения.
12. Виртуальные локальные сети (VLAN): принцип работы, тегирование (IEEE 802.1Q), назначение в сегментации сетей.
13. Основы сетевой безопасности для разработчика: изучение принципов работы сетевого экрана (брандмауэра), понятий DMZ и типовых сетевых атак (DoS, MITM).
14. Протокол HTTPS и технология TLS/SSL: изучение принципа шифрования, этапов handshake и роли сертификатов.
15. Сетевые сокеты (Sockets API): самостоятельное написание простейших клиентсерверных приложений на TCP и UDP на выбранном языке программирования.
16. Принципы RESTful API: изучение ограничений архитектуры, методов HTTP, кодов состояния и форматов данных (JSON/XML).
17. Веб-сокеты (WebSocket): изучение протокола, сравнение с HTTP для long-polling, реализация простого real-time приложения.
18. Работа с сетевыми библиотеками и фреймворками: изучение возможностей библиотек для сетевого взаимодействия на выбранном языке (например, requests для Python, HttpClient для .NET).

19. Контейнеризация и сети: изучение типов сетей Docker (bridge, host, none, overlay), создание пользовательской сети и настройка связей между контейнерами.
20. Беспроводные сети Wi-Fi: изучение стандартов (802.11n/ac/ax), методов аутентификации (WPA2-Personal, WPA2-Enterprise) и базовых принципов безопасности.
21. Протоколы удаленного управления: сравнение Telnet и SSH, практическое освоение настройки и использования SSH-ключей для аутентификации.
22. Основы облачных сетей (VPC - Virtual Private Cloud): изучение базовых компонентов (подсети, таблицы маршрутизации, интернет-шлюзы) на примере публичных облаков.
23. Системы контроля версий в сетевом контексте: освоение работы с удаленными репозиториями Git по протоколам SSH и HTTPS, разрешение конфликтов.
24. Мониторинг сетевых приложений: изучение ключевых метрик (latency, throughput, error rate) и базовых принципов настройки систем мониторинга (например, Prometheus + Grafana для метрик приложения).
25. Документирование сетевой архитектуры проекта: составление диаграмм развертывания (deployment diagram), описание используемых портов, протоколов и endpoints API.
26. Принципы балансировки нагрузки (Load Balancing): изучение целей, базовых алгоритмов (round-robin, least connections) и их влияния на архитектуру приложения.
27. Сетевые атаки на уровне приложения: изучение механизмов атак (SQL-инъекция, XSS) и способов защиты на стороне кода (валидация, экранирование, параметризованные запросы).
28. Основы отказоустойчивости и устойчивости сетевых сервисов: изучение паттернов (retry, circuit breaker, fallback) и их реализаций.
29. Автоматизация сетевых операций: написание скриптов (на Python/bash) для автоматической проверки доступности сервисов, сбора конфигурации или генерации отчетов.
30. Тенденции в сетевых технологиях: исследование концепций SDN (Software-Defined Networking), принципов сетей 5G и их потенциального влияния на разработку приложений.

Примерные варианты тестовых оценочных заданий (ТОЗ) для контрольного рубежа в рамках текущего контроля

Тестовое задание	Оцениваемые компетенции
ВОПРОСЫ ОТКРЫТОГО ТИПА	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Модель сетевого взаимодействия, описывающая семь уровней, называется _____. +: модель OSI	ОК 02.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Устройство, работающее на сетевом уровне и осуществляющее пересылку пакетов между разными сетями, называется _____. +: маршрутизатор +: router	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол, обеспечивающий надежную, соединение-ориентированную доставку данных на транспортном уровне, обозначается аббревиатурой _____. +: TCP	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Логическая группировка устройств в рамках одной физической сети для повышения безопасности и управления трафиком называется _____. +: VLA +: Virtual Local Area Network	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Технология, позволяющая нескольким устройствам в локальной сети использовать для выхода в интернет один публичный IP-адрес, называется _____. +: NAT +: Network Address Translation	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Утилита командной строки, используемая для проверки доступности	ОК 01.

сетевого узла по ICMP-запросам, называется _____. +: ping	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол безопасной передачи гипертекста, использующий шифрование TLS/SSL, обозначается аббревиатурой _____. +: HTTPS	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Основной программный интерфейс (API) для сетевого программирования, представляющий собой конечную точку для обмена данными, называется _____. +: сокет +: socket	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Принцип архитектуры веб-сервисов, основанный на использовании методов HTTP и стандартных кодов состояния, называется _____ API. +: REST +: Representational State Transfer	ОК 02.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Основной протокол динамического получения IP-адреса и других сетевых параметров в TCP/IP-сетях обозначается аббревиатурой _____. +: DHCP +: Dynamic Host Configuration Protocol	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Документ, описывающий набор методов (endpoints), которые предоставляет веб-сервис, их параметры и форматы данных, называется _____ API. +: спецификация	ОК 05.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс преобразования доменного имени (например, yandex.ru) в соответствующий IP-адрес называется _____. +: DNS-разрешение +: resolution	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Анализатор сетевого трафика, часто используемый для отладки и обучения, называется _____. +: Wireshark	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Сетевой протокол, используемый для автоматического обнаружения MAC-адреса по известному IP-адресу в локальной сети, называется _____. +: ARP +: Address Resolution Protocol	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Механизм, позволяющий веб-серверу поддерживать состояние пользовательской сессии между несколькими HTTP-запросами, обычно реализуется с помощью _____. +: cookie +: куки +: сессионных токенов	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ)	ОК 09.

Утилита командной строки, отображающая путь, который проходят пакеты до целевого узла, и задержки на каждом участке, в Windows называется _____. +: tracert	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Принцип, согласно которому сетевое приложение должно быть готово корректно обрабатывать ситуации потери пакетов, таймаутов соединения и недоступности сервисов, называется _____. +: отказоустойчивость +: resilience +: устойчивость к сбоям	ОК 01.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол, используемый для динамического обмена информацией о маршрутах между маршрутизаторами в рамках одной автономной системы, называется _____ (приведите общее название). +: IGP +: Interior Gateway Protocol +: OSPF +: RIP	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Специальный IP-адрес 127.0.0.1 зарезервирован для _____. +: петлевого интерфейса +: loopback +: обращения компьютера к самому себе	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Архитектурный стиль, при котором приложение состоит из множества небольших, слабо связанных и независимо развертываемых сервисов, называется _____. +: микросервисная архитектура +: microservices	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Для разделения одной физической сети на несколько изолированных широковещательных доменов на коммутаторах настраивают _____. +: VLAN +: Virtual Local Area Network	ОК 02.
ВОПРОСЫ ЗАКРЫТОГО ТИПА	
Какой из перечисленных протоколов является протоколом транспортного уровня? +: TCP -: HTTP -: IP -: ARP	ОК 01.
Какой IP-адрес относится к диапазону частных (private) адресов IPv4? +: 192.168.1.1 -: 8.8.8.8 -: 127.0.0.1 -: 169.254.10.5	ОК 02.
Что из перечисленного является ПРАВИЛЬНЫМ порядком инкапсуляции данных в модели TCP/IP? +: Данные приложения -> TCP-сегмент -> IP-пакет -> Ethernet-кадр -: Ethernet-кадр -> IP-пакет -> TCP-сегмент -> Данные приложения	ОК 02.
-: IP-пакет -> Ethernet-кадр -> TCP-сегмент -> Данные приложения -: TCP-сегмент -> Данные приложения -> Ethernet-кадр -> IP-пакет	

Какой метод HTTP используется для ЗАПРОСА данных с сервера (например, для получения веб-страницы)? +: GET -: POST -: PUT -: DELETE	ОК 09.
Какой инструмент командной строки в ОС Windows используется для ОТОБРАЖЕНИЯ текущей сетевой конфигурации (IP-адрес, маска, шлюз)? +: ipconfig -: ping -: tracert -: netstat	ОК 01.
Какой тип DNS-записи связывает доменное имя с IPv4-адресом? +: A-запись -: AAAA-запись -: CNAME-запись -: MX-запись	ОК 02.
Что является основной целью использования межсетевого экрана (брандмауэра)? +: Контроль и фильтрация сетевого трафика на основе заданных правил безопасности -: Ускорение передачи данных в локальной сети -: Автоматическое назначение IP-адресов устройствам -: Преобразование доменных имен в IP-адреса	ОК 01.
При разработке клиент-серверного приложения разработчик должен задокументировать используемые сетевые порты. К какому разделу проектной документации это относится? +: Архитектура системы и сетевые требования -: Руководство пользователя -: План тестирования -: Резюме проекта	ОК 05.
Какой протокол/технология используется для безопасного удаленного доступа к командной строке сервера? +: SSH (Secure Shell) -: Telnet -: FTP -: HTTP	ОК 09.

Шкала оценивания тестовых заданий

Данный вид контроля, рассчитан на выявление уровня усвоения теоретического и практического материала в рамках изучения дисциплин. Критерии оценивания теста: 1 вопрос = 1 балл.

Оценка «5»	30-27 Баллов
Оценка «4»	26-23 Баллов
Оценка «3»	22-18 Баллов
Оценка «2»	0-17 Баллов