Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 06.11.2026 17:39:38
Уникальный программный ключ:
637517d24e103c3db032acf37e839d98ec1c3bb2f3eb89c29abfcd7f43985447

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.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14 Компьютерные сети

Специальность
09.02.13 Интеграция решений с применением технологий искусственного интеллекта

Квалификация выпускника:
Специалист по работе с искусственным интеллектом

на базе основного общего образования

Форма обучения: очная

Москва

Фонд оценочных средств для дисциплины «ОП.14 Компьютерные сети». Специальность 09.02.13 Интеграция решений с применением технологий искусственного интеллекта квалификация: специалист по работе с искусственным интеллектом /– 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.14 Компьютерные сети» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «ОП.14 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. Какие ключевые требования к сети предъявляют системы распределенного обучения нейронных сетей (латенция, пропускная способность)?
2. Как архитектура кластера для высокопроизводительных вычислений (HPC) влияет на проектирование его сети?
3. Объясните, почему технология RDMA (Remote Direct Memory Access) критически важна для синхронизации градиентов между узлами при обучении моделей.
4. Сравните инфраструктурные преимущества и недостатки InfiniBand и высокоскоростного Ethernet (100/200/400 GbE) для дата-центра ИИ.
5. Как принципы программно-определяемых сетей (SDN) могут оптимизировать трафик в среде микросервисных ML-платформ?
6. Что такое «узкое место» в сети кластера и как его выявить при масштабировании тренировочных задач?
7. Опишите роль топологии сети (Fat-Tree, Dragonfly+) в обеспечении минимальной задержки между любыми вычислительными узлами.
8. Как сетевые протоколы транспортного уровня (настройки TCP/UDP) влияют на скорость передачи больших датасетов или чекпоинтов модели?
9. Какие сетевые технологии используются для реализации гибридного облака (Hybrid Cloud) при работе с чувствительными к задержкам ИИ-приложениями?
10. Объясните концепцию «вычисление в сети» (In-Network Computing) и ее потенциальное применение для агрегации данных в ML-пайплайнах.
11. Какие специфические сетевые угрозы актуальны для ИИ-систем (атаки на обучающие данные, кражу моделей, подмену API)?
12. Как архитектура микросегментации (Zero Trust) применяется для изоляции окружений разработки, обучения и продакшена ML-моделей?
13. Зачем для API инференса ML-моделей необходима настройка WAF (Web Application Firewall) и ограничение скорости запросов (Rate Limiting)?
14. Опишите процесс и инструменты для проведения сетевого аудита безопасности развернутой ML-платформы.
15. Как обеспечить конфиденциальность данных при их передаче по сети для федеративного обучения (Federated Learning)?
16. Что такое атаки типа «Adversarial» на сетевом уровне и как от них защищаться?
17. Каковы лучшие практики настройки групп безопасности (Security Groups) и сетевых политик в Kubernetes для изоляции подов с ИИ-сервисами?
18. Зачем использовать mTLS (mutual TLS) для аутентификации и шифрования трафика между микросервисами в распределенной ИИ-системе?
19. Как сетевые системы обнаружения вторжений (IDS/IPS) могут помочь в выявлении аномальной активности, связанной с попытками кражи модели?
20. Опишите модель угроз для Edge-ИИ системы, где данные передаются с периферийных устройств в центральное хранилище.
21. Сравните REST API и gRPC с точки зрения производительности и удобства для организации сервисов инференса ML-моделей.

22. Какой протокол (MQTT, AMQP, Kafka) и почему следует выбрать для построения событийно-ориентированного пайплайна обработки потоковых данных для ИИ?
23. Опишите роль API-шлюза (API Gateway) в архитектуре, состоящей из множества специализированных ML-микросервисов.
24. Как сервисная сеть (Service Mesh, напр., Istio) упрощает управление сетевым взаимодействием, безопасностью и наблюдаемостью в распределенных MLприложениях?
25. Для каких сценариев в ИИ оптимально использовать протокол HTTP/2 или HTTP/3 вместо HTTP/1.1?
26. Как работает и для чего используется **протокол NFS или SMB в контексте предоставления общего доступа к большим датасетам для тренировочных узлов?
27. Объясните, как Kubernetes Service (типы ClusterIP, NodePort, LoadBalancer) обеспечивает сетевое взаимодействие с подом, в котором запущен контейнер с MLмоделью.
28. Что такое Kubernetes Ingress и как он используется для маршрутизации внешнего HTTPS-трафика к различным сервисам инференса?
29. Как протоколы облачных провайдеров (AWS S3 API, Google Cloud Storage API) используются для взаимодействия с данными в гибридных ML-сценариях?
30. Опишите принцип работы и применение P2P (peer-to-peer) сетей для децентрализованного обучения или обновления моделей.
31. Какие метрики сетевого мониторинга (латентность, джиттер, потеря пакетов, использование полосы) наиболее важны для SLA ML-сервиса реального времени?
32. Как сжатие данных (gzip, snappy) на сетевом уровне может ускорить передачу больших тензоров или датасетов?
33. Что такое TCP BBR и как этот алгоритм управления перегрузкой может улучшить пропускную способность для потоковой передачи данных обучения?
34. Как использовать приоритизацию сетевого трафика (QoS) для обеспечения минимальной задержки для трафика инференса при наличии фоновых задач (например, загрузки данных)?
35. Опишите процесс профилирования сетевых затрат в распределенном тренировочном запуске с помощью инструментов вроде NVIDIA NCCL.
36. Какие инструменты (Prometheus, Grafana, специализированные дашборды cloudпровайдеров) использовать для мониторинга сетевой инфраструктуры ИИплатформы?
37. Что такое NetDevOps и как его практики (IaC для сетей) применяются для управления сетевыми конфигурациями в CI/CD пайплайнах развертывания MLмоделей?
38. Как организовать георезервирование (Geo-Redundancy) и аварийное переключение (Failover) сетевых сервисов для глобально доступного ML-API?
39. Опишите стратегию кэширования сетевых ответов (например, с помощью CDN или Redis) для часто запрашиваемых результатов инференса.
40. Как автоматическое масштабирование (Autoscaling) сетевых балансировщиков нагрузки и бэкенд-сервисов помогает справляться с пиковым спросом на MLсервис?
41. Спроектируйте логическую сетевую схему для гибридной системы, где тренировка идет в облаке, а инференс — на edge-устройствах. Какие протоколы и технологии связи использовать?

42. Как построить сеть для федеративного обучения, обеспечив безопасный обмен только обновлениями моделей между множеством участников?
43. Опишите архитектуру сети для системы автономного вождения, где требуется сверхнизкая задержка связи между автомобилями (V2V) и инфраструктурой (V2I).
44. Какие сетевые инновации (оптические коммутаторы, квантовые сети) могут кардинально изменить производительность распределенных ИИ-систем в будущем?
45. Как технологии 5G/6G и сети с резервированием ресурсов (Network Slicing) повлияют на развертывание ИИ-сервисов с детерминированными требованиями к задержке?
46. Что такое AI for Networks (AIN) и как машинное обучение используется для оптимизации работы самих компьютерных сетей (прогноз трафика, автоматическое устранение неисправностей)?
47. Как организовать сетевое взаимодействие в рамках платформы MLOps между хранилищем данных, средами для экспериментов, registry моделей и сервисами инференса?
48. Опишите проблемы безопасности и пути их решения при передаче данных для мультимодальных ИИ-моделей (текст, изображение, аудио) по сети.
49. Какие стандарты и протоколы (ONNX Runtime, TensorFlow Serving API) являются де-факто для сетевого взаимодействия с моделями различных фреймворков?
50. Проанализируйте кейс: после развертывания новой версии модели резко возросла сетевая задержка инференса. Каков алгоритм диагностики и поиска узкого места?

Темы для самостоятельной работы обучающихся

1. Требования к сетевой инфраструктуре для распределенного обучения моделей (Data Parallelism, Model Parallelism).
2. Протоколы и технологии для синхронизации градиентов между узлами кластера (gRPC, MPI, NCCL).
3. Сравнение сетевых технологий RDMA (RoCE, InfiniBand) и TCP/IP для высоконагруженных ML-пайплайнов.
4. Архитектура и настройка высокоскоростных сетей в дата-центрах для HPC/ИИ (Fat-Tree, Dragonfly+).
5. Сетевые аспекты развертывания ML-микросервисов в Kubernetes (Service, Ingress, Network Policies).
6. Обеспечение низкой задержки (low-latency) для инференс-сервисов ИИ в реальном времени.
7. Оптимизация передачи больших датасетов по сети: выбор протоколов, сжатие данных, тюнинг TCP.
8. Модели угроз и защита API машинного обучения от сетевых атак (DoS, инъекции, перехват).
9. Применение принципов Zero Trust Network Access (ZTNA) для изоляции сред разработки и продакшена ИИ.
10. Использование балансировщиков нагрузки (L4/L7) для масштабирования сервисов инференса.
11. Сетевые протоколы для IoT/Edge-устройств, передающих данные для обработки ИИ (MQTT, CoAP).
12. Организация защищенных каналов (VPN, IPsec, WireGuard) для федеративного обучения (Federated Learning).

13. Мониторинг сетевых метрик (латентность, джиттер, потери) в распределенных ИИсистемах.
14. Влияние сетевой конфигурации на производительность фреймворков распределенного обучения (PyTorch DDP, TensorFlow TF_CONFIG).
15. Сетевые требования и архитектура для систем автономного вождения (V2Xкоммуникация).
16. Проектирование отказоустойчивой сетевой инфраструктуры для критичных ИИсервисов.
17. Использование CDN для распределения весов моделей и датасетов в глобальных ML-системах.
18. Анализ сетевого трафика ML-платформ для выявления аномалий и узких мест.
19. Настройка QoS (Quality of Service) для приоритизации трафика инференса над фоновыми задачами.
20. Сетевые аспекты MLOps: автоматизация развертывания сетевых конфигураций для новых моделей.
21. Безопасность передачи обучающих данных между облачными и локальными (onpremise) центрами.
22. Протоколы и практики для организации peer-to-peer сетей в децентрализованном машинном обучении.
23. Оптимизация сетевого стека ОС (Linux kernel tuning) для высокопроизводительных ML-вычислений.
24. Использование SmartNIC и DPU для оффлоада сетевых операций в серверах ИИ.
25. Сетевые требования для мультимодальных ИИ-систем, обрабатывающих видео, аудио и текст.
26. Проектирование гибридных сетей (cloud + edge) для распределенных ИИприложений.
27. Сетевые инструменты для диагностики проблем производительности в распределенном тренировочном запуске.
28. Аутентификация и авторизация для доступа к ML-API с использованием сетевых токенов (JWT, OAuth).
29. Применение технологий SDN (Software-Defined Networking) для динамического управления трафиком в дата-центре ИИ.
30. Особенности сетевого взаимодействия при использовании графовых нейронных сетей (GNN) на распределенных данных.
31. Обеспечение конфиденциальности данных в сети для приватного машинного обучения (Private ML).
32. Сетевые паттерны для event-driven архитектур в ИИ-системах (Kafka, RabbitMQ).
33. Влияние выбора облачного провайдера (AWS, GCP, Azure) на сетевую архитектуру ML-решения.
34. Оптимизация сетевых затрат при передаче больших объемов данных между Availability Zones/Regions.
35. Использование протокола HTTP/3 (QUIC) для улучшения взаимодействия с MLсервисами в нестабильных сетях.
36. Сетевые аспекты развертывания больших языковых моделей (LLM) как сервиса.
37. Организация зеркалирования и репликации моделей и данных между географически распределенными ЦОД.

38. Сетевые требования для систем компьютерного зрения реального времени (видеоаналитика).
39. Применение сетевых функций виртуализации (NFV) для создания гибких сервисных цепочек в ИИ-платформах.
40. Анализ уязвимостей в сетевых API популярных фреймворков машинного обучения (TensorFlow Serving, TorchServe).
41. Проектирование сети для обучения с подкреплением (RL) в распределенной симуляционной среде.
42. Сетевые инструменты и методики для нагрузочного тестирования (load testing) MLэндпоинтов.
43. Обеспечение соответствия сетевым стандартам и регуляториям (GDPR, HIPAA) при обработке данных ИИ.
44. Использование P2P-сетей для распределенной агрегации обновлений моделей (децентрализованное обучение).
45. Сетевые стратегии для минимизации задержки в системах рекомендаций (recommendation systems) в реальном времени.
46. Миграция сетевой инфраструктуры ИИ-платформы при переходе с монолитной на микросервисную архитектуру.
47. Применение машинного обучения для анализа и оптимизации сетевого трафика (AI for Networks).
48. Сетевые протоколы для управления распределенными вычислительными ресурсами в кластерах ИИ (Slurm, Kubernetes).
49. Обеспечение сетевой связности и безопасности для ИИ-сервисов, развернутых в гибридном облаке.
50. Тенденции развития сетевых технологий (оптические сети, квантовые коммуникации) и их влияние на будущее распределенного ИИ.

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

Тестовое задание	Оцениваемые компетенции
ВОПРОСЫ ОТКРЫТОГО ТИПА	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Основной сетевой протокол, обеспечивающий доставку данных с гарантией целостности и порядка пакетов, называется _____. +: TCP	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Уникальный числовой идентификатор устройства в локальной сети, назначаемый производителем, называется _____ адресом. +: MAC	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Сетевой протокол, преобразующий доменные имена в IP-адреса, называется _____. +: DNS	ОК 01.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Логическое разделение одной физической сети на несколько независимых широковещательных доменов осуществляется с помощью технологии _____. +: VLAN	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол, используемый для безопасного удаленного управления серверами и сетевым оборудованием по зашифрованному каналу, называется _____. +: SSH	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол динамического назначения IP-адресов устройствам в сети обозначается аббревиатурой _____. +: DHCP	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Основная задача сетевого _____ — фильтрация входящего и исходящего трафика на основе заданных правил безопасности. +: межсетевого экрана +: брандмауэра	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Технология, позволяющая объединить несколько физических	ОК 02.

сетевых каналов в один логический для увеличения пропускной способности и отказоустойчивости, называется _____. +: агрегацией каналов +: Link Aggregation	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол маршрутизации, используемый для обмена информацией о доступных сетях между маршрутизаторами в интернете, называется _____. +: BGP +: Border Gateway Protocol	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) В модели OSI процесс инкапсуляции данных пользователя для передачи по сети начинается на _____ уровне. +: прикладном +: application +: Application	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Принцип сетевой архитектуры, при котором доступ к ресурсам предоставляется только после проверки подлинности каждого запроса, независимо от его источника, называется _____. +: Zero Trust +: нулевое доверие	ПК 1.1.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Специализированный протокол для передачи метрик и состояния сетевых устройств в системы мониторинга называется _____. +: SNMP	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Механизм балансировки сетевой нагрузки, работающий на транспортном уровне модели OSI (L4), распределяет запросы на основе IP-адреса и номера _____. +: порта	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Для подключения и настройки сетевого интерфейса в операционных системах Linux используется команда _____. +: ip +: ifconfig	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Атака на отказ в обслуживании, при которой злоумышленник использует множество скомпрометированных устройств для генерации трафика, называется _____ атакой. +: DDoS	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Программный интерфейс (API) для взаимодействия с сетевыми функциями в операционных системах семейства Windows называется _____. +: Winsock +: Windows Sockets	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Набор правил, определяющий, какой сетевой трафик разрешен или запрещен между сегментами сети в Kubernetes, называется _____.	ПК 1.1.
+: NetworkPolicy	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Утилита командной строки, используемая для проверки возможности обмена сетевыми пакетами с удаленным хостом, называется _____. +: ping	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол, обеспечивающий безопасный обмен ключами шифрования для установления защищенного VPN-соединения (такого как IKEv2), называется _____. +: IKE +: Internet Key Exchange	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Сетевой порт, используемый протоколом HTTPS для защищенного веб-соединения по умолчанию, — это порт _____. +: 443	ПК 1.1.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Глобальная компьютерная сеть, объединяющая миллионы устройств по всему миру и использующая протокол TCP/IP для передачи данных, называется _____. +: Интернет	ПК 1.1.
ВОПРОСЫ ЗАКРЫТОГО ТИПА	
Какой уровень модели OSI отвечает за логическую адресацию и маршрутизацию пакетов между разными сетями? +: Сетевой (Network) -: Канальный (Data Link) -: Транспортный (Transport) -: Физический (Physical)	ОК 01.
Что из перечисленного НЕ является типом IP-адреса по версии IPv4? +: FEC0::1 (это IPv6) -: 192.168.1.1 -: 10.0.0.1 -: 172.16.0.1	ОК 01.
Какой протокол/технология используется для предотвращения петель (loops) в сетях с избыточными связями на канальном уровне? +: STP (Spanning Tree Protocol) -: OSPF (Open Shortest Path First) -: ARP (Address Resolution Protocol) -: DNS (Domain Name System)	ОК 01.
Что такое маска подсети (subnet mask)? +: Число, определяющее, какая часть IP-адреса относится к адресу сети, а какая — к адресу хоста. -: Фильтр для блокировки нежелательного трафика. -: Адрес шлюза по умолчанию. -: Пароль для доступа к сети.	ОК 01.
Какой протокол является протоколом состояния каналов (link-state protocol) для маршрутизации внутри одной автономной системы? +: OSPF (Open Shortest Path First) -: BGP (Border Gateway Protocol) -: RIP (Routing Information Protocol) -: EIGRP (Enhanced Interior Gateway Routing Protocol)	ОК 02.
Что из перечисленного является основным назначением протокола	ОК 02.
ARP? +: Определение MAC-адреса по известному IP-адресу в локальной сети. -: Преобразование доменного имени в IP-адрес. -: Динамическое назначение IP-адреса устройству. -: Шифрование сетевого трафика.	
Какая утилита позволяет просмотреть таблицу маршрутизации в операционной системе Windows? +: route print -: ipconfig /all -: tracert -: netstat -an	ОК 02.

Какой стандарт описывает технологию Ethernet со скоростью 1000 Мбит/с (Гигабитный Ethernet)? +: IEEE 802.3ab -: IEEE 802.11ac -: IEEE 802.3u -: IEEE 802.1Q	ОК 02.
Что такое «порт» в контексте сетевых технологий? +: Числовой идентификатор, используемый транспортными протоколами для определения приложения или службы. -: Физический разъем на сетевом устройстве. -: Скорость передачи данных в сети. -: Тип сетевого кабеля.	ОК 02.

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