

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

ПМ.03 Эксплуатация облачных сервисов

09.02.06 Сетевое и системное администрирование

Форма обучения очная

Владивосток 2026

Рабочая программа профессионального модуля разработана в соответствии с требованиями Федерального государственного стандарта среднего профессионального образования по специальности среднего профессионального образования программы подготовки специалистов среднего 09.02.06 Сетевое и системное администрирование, утвержденного приказом Минпросвещения России от 10.07.2023 №519.

Разработана:

Реуцкий Р.С., преподаватель Колледжа сервиса и дизайна ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от « 18 » 05 2026 г.

Председатель ЦМК  Е.А. Стефанович
подпись

подпись

Согласована:

Начальник отдела информационных технологий, Филиал Российской телевизионной и радиовещательной сети «Приморский краевой радиотелевизионный передающий центр»


(подпись, печать) Д.М. Шумов


СОДЕРЖАНИЕ

1	Общая характеристика рабочей программы	4
2	Структура и содержание профессионального модуля	6
3	Условия реализации программы модуля	23
4	Контроль и оценка результатов освоения профессионального модуля (вида профессиональной деятельности)	24

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 УЧАСТИЕ В ПРОЕКТИРОВАНИИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее – программа ПМ) - является частью программы подготовки специалистов среднего звена по специальности СПО 09.02.06 Сетевое и системное администрирование.

Рабочая программа составляется для студентов очной формы обучения.

1.2. Требования к результатам освоения модуля:

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности «Эксплуатация облачных сервисов», в том числе общими компетенциям (ОК) и профессиональными компетенциями (ПК), указанными в ФГОС по специальности 09.02.06 Сетевое и системное администрирование.

1.2.1 Перечень профессиональных компетенций

Код	Наименование видов деятельности п профессиональных компетенций
ПК 3.1	Осуществлять развертывание облачной инфраструктуры
ПК 3.2	Проводить документирование требований и технических возможностей облачных инфраструктур
ПК 3.3	Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки
ПК 3.4	Производить хранение и анализ данных
ПК 3.5	Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов
ПК 3.6	Проводить мониторинг системы в облачных сервисах

1.2.2 Базовая часть

С целью овладения видом профессиональной деятельности эксплуатация облачных сервисов и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

Владеть навыками	в развертывании облачной инфраструктуры; настройке балансировщиков нагрузки и проведения тестирования жизнеспособности облачных сервисов; реализации концепции декларативного управления инфраструктурой; организации документирования технических требований к облачным инфраструктурам; создания и поддержки планов автоматического масштабирования; создания образов виртуальных машин; управления образами виртуальных машин; организации распределения нагрузки внутри облачно инфраструктуры; организации хранения данных в облачной инфраструктуре; проведения анализа данных; обеспечения безопасности в облачной инфраструктуре;
------------------	--

	организации функции управления учетными записями и доступом к облачной инфраструктуре; настройки службы защиты сетей от внешних атак; маркировки ресурсов для последующего мониторинга и оценки стоимости; сбора метрик и формирования журнала мониторинга; внедрения и осуществления мониторинга облачных сервисов;
Уметь	определять общие модели развертывания облачной инфраструктуры; поддерживать облачные конфигурации в актуальном состоянии и вести учет контроля версий; определять, насколько данные модели соответствуют требованиям, специфичным для организации; пользоваться преимуществами облачной инфраструктуры для снижения операционных нагрузок при развертывании служб; документировать ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру; переводить бизнес-цели и задачи в спецификации, а также презентовать их заинтересованным сторонам; проводить оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности; создавать внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака; проводить оценку, выбирать и внедрять базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище; разрабатывать и внедрять процессы проверки подлинности на уровне подразделения и компании в целом, контролировать доступ к системе управления общедоступным облаком. анализировать и интерпретировать показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре; использовать методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов; реализовать стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров; внедрять базы данных и решения для хранения данных, которые наилучшим образом соответствуют потребностям конкретного приложения; разрабатывать и внедрять процессы проверки подлинности на уровне подразделения и компании в целом, контролировать доступ к системе управления общедоступным облаком;

	использовать общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости; проводить постоянные проверки отказоустойчивости и восстановления системы; внедрение решений для мониторинга с целью формирования предупреждений и автоматизации реагирования на различные инциденты; поддерживать облачные конфигурации в актуальном состоянии и вести учет контроля версий; внедрять централизованный сбор и анализ метрик для системной, сетевой и прикладной информации; проводить постоянные проверки отказоустойчивости и восстановления системы;
Знать	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами; разграничение ответственности за безопасность между поставщиком облачных услуг и клиентом публичного облака; показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры; требования к совместимости компонентов внутри облачной инфраструктуры; сетевой поток данных и соответствующая зависимость доступности систем; методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам; разграничение ответственности за безопасность между поставщиком облачных услуг и клиентом публичного облака; различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками; как взаимодействовать с бизнес-единицами для определения лучших практик развертывания и создания плана по миграции в облачную инфраструктуру; важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений; различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами. основные потребности инфраструктурного дизайна для отдельных групп инженеров; различные технологические решения для достижения бизнес-целей; сетевой поток данных и соответствующая зависимость доступности систем; требования к производительности и возможные узкие места при проектировании инфраструктуры; важность каждого уровня инфраструктуры, включая вычисление, хранение,

	сетевое взаимодействие, базы данных, использование кэша и приложений; различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами; показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры; методики и возможности автоматизации, широко используемые в техническом сообществе; методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам; важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений; требования к совместимости компонентов внутри облачной инфраструктуры; методики и возможности автоматизации, широко используемые в техническом сообществе; сетевой поток данных и соответствующая зависимость доступности систем; требования к производительности и возможные узкие места при проектировании инфраструктуры; различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами; важность и назначение сетевого трафика, а также изоляцию ресурсов; различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками; сетевой поток данных и соответствующая зависимость доступности систем; как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур; требования к производительности и возможные узкие места при проектировании инфраструктуры;
--	---

1.2.3 Количество часов, отводимое на освоение профессионального модуля

Всего часов 826

Из них на освоение МДК.01.01 170

на освоение МДК.01.02 172

на освоение МДК.01.03 226

на практики 492, в том числе учебную 108, производственную (по профилю специальности) 144.

экзамен по модулю 6.

2.1. Структура профессионального модуля

Форма аттестации МДК.03.01 – дифференцированный зачет;
Форма аттестации МДК.03.02 – экзамен;
Форма аттестации МДК 03.03 – экзамен;
Форма аттестации УП – дифференцированный зачет;
Форма аттестации ПП (по профилю специальности) – дифференцированный зачет;
Форма аттестации ПМ.03 – экзамен квалификационный.

**2.2. Тематический план и содержание профессионального модуля)
ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект		Объём в часах
1	2		3
Раздел 1. Технологии виртуализации и автоматизации			120/74
МДК.03.01. Технологии виртуализации и автоматизации			120/74
Тема 1.1. Виртуализация и основы облачных технологий	Содержание		16
	1	Введение в виртуализацию Понятие и назначение виртуализации. Аппаратная и программная виртуализация. Преимущества и ограничения.	
	2	Типы гипервизоров Гипервизоры типа 1 и 2. Примеры: VMware ESXi, Hyper-V, KVM. Сравнительный анализ.	
	3	Виртуальные ресурсы Виртуальные процессоры, память, диски, сетевые адаптеры. Принципы распределения и балансировки нагрузки.	
	4	Виртуальная сеть и коммутация Сетевые мосты, виртуальные коммутаторы, NAT. Настройка маршрутизации между виртуальными машинами.	
	5	Инструменты виртуализации QEMU, KVM, Virt-manager. Создание и управление виртуальными машинами, снимки, клонирование, миграции.	
	6	Кластеризация и отказоустойчивость Принципы построения кластеров. Репликация и балансировка нагрузки. Обзор Proxmox VE.	
	7	Интеграция виртуализации и сетевого администрирования виртуальные сети, VLAN, маршрутизация, управление доступом. Практические аспекты безопасности.	
	8	Обзор облачных платформ Введение в понятие облака. Переход от виртуализации к облачным технологиям. Примеры решений: OpenStack, Proxmox, VMware Cloud.	
	Практические занятия		28
	1.1.1	Установка и настройка Hosted-гипервизора: Установка VirtualBox или VMware Workstation. Настройка сети NAT и Host-Only.	

	1.1.2	Установка нативного гипервизора: Развёртывание KVM или Proxmox VE на физическом сервере.	
	1.1.3	Создание и управление виртуальными машинами: Создание, копирование, клонирование, импорт/экспорт VM.	
	1.1.4	Настройка виртуальной маршрутизации и сетей: Создание виртуальных мостов, VLAN, NAT, настройка маршрутов.	
	1.1.5	Автоматизация развёртывания виртуальных машин: Использование шаблонов VM, Cloud-init или Ansible для автоматической настройки.	
	1.1.6	Конфигурация ресурсов виртуальных машин: Изменение параметров CPU, RAM, дисков, сетей. Управление приоритетами.	
	1.1.7	Резервное копирование и миграция виртуальных машин: Создание снимков, восстановление, live migration в Proxmox VE.	
	1.1.8	Создание отказоустойчивого кластера в Proxmox VE: Настройка двух узлов с репликацией и failover.	
	1.1.9	Мониторинг и управление кластером: Использование встроенных инструментов Proxmox для отслеживания состояния VM.	
	1.1.10	Развёртывание базовых сервисов внутри VM: Установка LAMP, FTP или DNS-сервера. Проверка сетевой доступности.	
	1.1.11	Развёртывание сервисов конечного пользователя: Настройка HostPanel, базы данных, службы аутентификации.	
	1.1.12	Создание изолированной виртуальной сети: Настройка внутренней сети для тестирования сервисов.	
	1.1.13	Мини-проект: виртуализированная инфраструктура кампуса: Студент моделирует схему сети из нескольких VM и настраивает взаимодействие между ними.	
Тема 1.2. Контейнеризация и оркестрация сервисов	Содержание		16
	1	Контейнеризация как развитие виртуализации Отличия контейнеров от виртуальных машин. Преимущества контейнеризации.	
	2	Архитектура Docker Docker Engine, Registry, Image, Container. Управление образами и контейнерами.	
	3	Docker Compose и многоконтейнерные приложения Файлы docker-compose.yml, настройка сетей, томов и сервисов.	
	4	Основы Kubernetes Компоненты: master, node, pod, service. Принцип работы etcd, kubelet, kube-proxy.	
	5	Управление приложениями в Kubernetes	

		kubectl, Deployment, ReplicaSet, ConfigMap, Secret. Принципы масштабирования и обновления.	
	6	Планирование и распределение ресурсов Планировщик, приоритизация, вытеснение, QoS.	
	7	Сбор логов и мониторинг Основы логирования и наблюдения в Kubernetes. Архитектура сбора логов на уровне узлов и кластера.	
	8	Резервное копирование и миграции контейнеров Снимки, восстановление, перенос сервисов между узлами и кластерами.	
	Практические занятия		28
	1.2.1	Введение в Docker и контейнеризацию: Установка Docker Engine, создание первого контейнера.	
	1.2.2	Работа с образами Docker: Создание собственного Dockerfile, публикация образа.	
	1.2.3	Управление контейнерами и томами: Подключение томов, монтирование данных, настройка сетей контейнеров.	
	1.2.4	Многоконтейнерные приложения с Docker Compose: Развёртывание web-приложения (Nginx + PHP + DB).	
	1.2.5	Установка Kubernetes в среде Proxmox VE: Создание кластера Kubernetes на 2–3 узлах.	
	1.2.6	Настройка Kubernetes и деплой приложения: Развёртывание подов, сервисов и ingress.	
	1.2.7	Оркестрация контейнеров Kubernetes: Репликация, масштабирование и автообновления приложений.	
	1.2.8	Работа с kubectl: Основные команды, получение статуса узлов и подов.	
	1.2.9	Мониторинг и логирование контейнеров: Настройка Fluent Bit, Prometheus или встроенного log-доступа.	
	1.2.10	Настройка отказоустойчивости и балансировки: Создание LoadBalancer и NodePort сервисов.	
	1.2.11	Сетевые политики и безопасность подов: Настройка NetworkPolicy для ограничения трафика.	
	1.2.12	Резервное копирование и восстановление контейнеров: Работа с Velero, сохранение состояния и восстановление приложения.	
	1.2.13	Мини-проект: кластерная среда для корпоративного портала: Развёртывание корпоративного портала в Kubernetes с балансировкой и логированием.	
Тема 1.3. Облачные сервисы и безопасность инфраструктуры	Содержание		14
	1	Модели облачных сервисов IaaS, PaaS, SaaS – принципы, различия, примеры реализации.	
	2	Облачные бизнес-модели	

		Экономика облачных решений, гибкие модели оплаты, примеры коммерческих облаков.	
3		Безопасность виртуальной инфраструктуры Изоляция пользователей, контроль доступа, разграничение прав, защита API.	
4		Сетевая безопасность в облаках Безопасная маршрутизация, VPN, firewall, сегментация и политики безопасности.	
5		Мониторинг и аудит Системы наблюдения за инфраструктурой, журналирование, анализ логов, реагирование на инциденты.	
6		Резервирование и восстановление после сбоев Стратегии Disaster Recovery, резервное копирование, тестирование восстановления сервисов.	
7		Практическая интеграция безопасности и оркестрации Обеспечение безопасности контейнеров и виртуальных машин в единой инфраструктуре.	
		Практические занятия	18
1.3.1		Введение в облачные бизнес-модели (IaaS, PaaS, SaaS): Работа с примерами публичных облаков (AWS, Yandex Cloud).	
1.3.2		Развёртывание IaaS в локальной среде: Настройка виртуальной инфраструктуры как услуги в Proxmox/OpenStack.	
1.3.3		Автоматизация IaaS-развёртывания: Использование Terraform или Ansible для создания VM по шаблону.	
1.3.4		Балансировщик нагрузки виртуальных машин: Настройка HAProxy или Nginx Load Balancer.	
1.3.5		PaaS: настройка платформы для web-приложений: Развёртывание контейнерного PaaS (например, Dokku, Portainer).	
1.3.6		SaaS: настройка облачного приложения: Развёртывание Nextcloud, мониторинг, резервирование данных.	
1.3.7		Контроль доступа и авторизация в облачной инфраструктуре: Создание ролей, управление ключами, политика доступа.	
1.3.8		Мониторинг и аудит событий безопасности: Анализ логов, настройка оповещений, журналирование.	
1.3.9		Финальный мини-проект: безопасная облачная инфраструктура организации: Проект объединяет виртуализацию, контейнеризацию и безопасность в единой системе.	
Самостоятельная работа при изучении раздела 1 ПМ.03 1. Изучение типов гипервизоров и принципов их работы. 2. Подготовка сервера для установки гипервизора. Анализ требований к оборудованию. 3. Создание и настройка виртуальных машин. Управление вычислительными ресурсами.			50

4. Изучение типов виртуальных сетей: NAT, мост, внутренние сети. 5. Настройка маршрутизации и сетевых интерфейсов в виртуальной среде. 6. Изучение механизмов резервного копирования и миграции виртуальных машин. 7. Изучение принципов построения кластеров Proxmox VE. Репликация и отказоустойчивость. 8. Развёртывание и настройка базовых серверных сервисов в виртуальной среде (DNS, FTP, LAMP). 9. Анализ механизмов изоляции и защиты сетей виртуальных машин. 10. Изучение принципов контейнеризации. Сравнение Docker и виртуальных машин. 11. Работа с Docker: создание, запуск и управление контейнерами. 12. Изучение структуры Dockerfile и создание собственных образов. 13. Использование Docker Compose для управления многоконтейнерными приложениями. 14. Изучение архитектуры Kubernetes и его основных компонентов. 15. Установка и настройка кластера Kubernetes. 16. Управление деплоями, сервисами и масштабированием в Kubernetes. 17. Настройка сетевых политик и балансировщиков нагрузки в Kubernetes. 18. Изучение систем логирования и мониторинга контейнеров (Prometheus, Grafana, Fluent Bit). 19. Анализ моделей облачных сервисов IaaS, PaaS, SaaS. 20. Изучение платформ для развёртывания IaaS (Proxmox Cloud, OpenStack). 21. Изучение принципов инфраструктуры как кода (IaC). Знакомство с Terraform и Ansible. 22. Анализ примеров PaaS и SaaS-сервисов. Практическое применение Portainer и Nextcloud. 23. Изучение средств защиты соединений в облаке. Настройка VPN и SSL-сертификатов. 24. Изучение моделей разграничения прав доступа (RBAC, ACL) в Kubernetes и виртуальных средах. 25. Подготовка отчёта и проектной документации по построению безопасной облачной инфраструктуры.		
Консультации по разделу 1 ПМ.03		
Экзамен по разделу 1 ПМ.03		
Раздел 2. Безопасность облачных сервисов		120/74
МДК.03.02. Безопасность облачных сервисов		120/74
Тема 2.1. Основы и архитектура безопасности облачных сервисов	Содержание	
	1	Понятие и особенности безопасности облачных сервисов Определение, задачи и цели защиты данных в облаке
	2	Модели ответственности (Shared Responsibility Model) Роли провайдера и клиента, примеры
	3	Основные угрозы и уязвимости облачных сервисов Классификация угроз, CVE, NVD
	4	Стандарты и нормативные требования ISO/IEC 27017, 27018, GDPR, ФЗ-152
		14

	5	Архитектура облачной безопасности Защита данных, сетей, пользователей, приложений	24
	6	Защита данных, сетей, пользователей, приложений MFA, RBAC, OAuth2, OpenID Connect, SAML	
	7	Технологии шифрования данных Технологии шифрования данных при хранении и передаче (SSL/TLS, AES, PGP)	
	Практические занятия		
	2.1.1	Модели облачных сервисов: Анализ IaaS, PaaS, SaaS. Определение зон ответственности	
	2.1.2	Анализ угроз облачных сервисов: Работа с базами уязвимостей (CVE, NVD)	
	2.1.3	Настройка MFA: Подключение многофакторной аутентификации для пользователей	
	2.1.4	Создание пользователей и ролей: Настройка RBAC, проверка разграничения прав	
	2.1.5	Шифрование данных: Настройка SSL/TLS, работа с сертификатами	
	2.1.6	Создание защищённого канала: Настройка PKI и VPN соединений	
	2.1.7	Подготовка схемы облачной архитектуры: Обозначение точек уязвимости, построение схемы	
	2.1.8	Резервное копирование данных: Настройка snapshot и restore виртуальных машин	
	2.1.9	Контроль целостности данных: Проверка checksum, хэш-функции	
	2.1.10	Аудит базовых настроек безопасности: Составление отчета по проверке облачного сервиса	
Тема 2.2. Технологии защиты и устойчивость инфраструктуры	Содержание		16
	1	Безопасность виртуальных машин и контейнеров Контейнеризация, изоляция, настройка доступа	
	2	Сетевые политики и сегментация VLAN, Security Groups, Firewall, NAT	
	3	VPN и защищённые соединения IPsec, WireGuard, SSL-VPN	
	4	Защита от DoS и DDoS атак Rate limit, Fail2Ban, Cloudflare, WAF	
	5	Системы мониторинга и IDS/IPS Suricata, Snort, WAF, логирование	
		Централизованный сбор логов ELK, Grafana Loki, аудит событий	
		Резервное копирование и восстановление данных Snapshot, репликация, Disaster Recovery	
		Обеспечение высокой доступности HAProxy, Keepalived, балансировка нагрузки	

	Практические занятия		26
	2.2.1	Настройка сегментации сети: Создание VLAN и межсетевых сегментов	
	2.2.2	Правила firewall для облачной сети: Правила firewall для облачной сети	
	2.2.3	Настройка NAT и VPN: Подключение защищённых туннелей между сегментами	
	2.2.4	Конфигурация IDS/IPS: Настройка Suricata или Snort для обнаружения атак	
	2.2.5	Централизованный сбор логов: Настройка ELK или Grafana Loki	
	2.2.6	Анализ журналов безопасности: Выявление подозрительных событий	
	2.2.7	Настройка защиты от DoS/DDoS: Rate limiting, Fail2Ban, Cloudflare	
	2.2.8	Настройка резервного копирования: Репликация данных, инкрементальные бэкапы	
	2.2.9	Настройка высокой доступности: HAProxy, Keepalived, балансировка нагрузки	
	2.2.10	Тестирование Disaster Recovery: Проверка восстановления сервисов	
	2.2.11	Мониторинг состояния инфраструктуры: Настройка Prometheus/Grafana	
	2.2.12	Настройка политики хранения логов: Автоматическая ротация и архивирование	
Тема 2.3. Управление доступом и эксплуатация защищённых решений	Содержание		16
	1	Политики доступа и IAM Создание пользователей, разграничение прав, RBAC	
	2	Развёртывание инфраструктуры IaaS, PaaS, SaaS Настройка сервисов, безопасная эксплуатация	
	3	Тестовые и изолированные среды Sandbox для тестирования новых версий ПО	
	4	DevSecOps и безопасность CI/CD Интеграция сканирования уязвимостей, автоматизация	
	5	Методы тестирования безопасности Vulnerability Scanning, Pentest, OWASP Top 10	
	6	Реагирование на инциденты Incident Response Workflow, уведомления	
	7	Документирование политики безопасности Создание документов, планов реагирования	
	8	Проектирование защищённой облачной инфраструктуры Объединение знаний из всех тем, комплексный кейс	
	Практические занятия		24
	2.3.1	Создание политики IAM: Настройка пользователей и ролей	
	2.3.2	Разграничение прав в Kubernetes / Proxmox: Практика RBAC	
	2.3.3	Развёртывание тестовой среды (sandbox): Изолированная среда для проверки ПО	
	2.3.4	Безопасный конвейер CI/CD: Настройка сканирования уязвимостей	
	2.3.5	Сканирование контейнеров: Trivy, Clair, проверка образов	

	2.3.6	Vulnerability Scanning: Анализ и устранение уязвимостей	
	2.3.7	Проведение pentest облачного сервиса: Использование OWASP Top 10	
	2.3.8	Реагирование на инциденты: Практика Incident Response Workflow	
	2.3.9	Настройка уведомлений и алертов: Автоматические оповещения о событиях	
	2.3.10	Документирование политики безопасности: Создание шаблонов и регламентов	
	2.3.11	Проверка соответствия стандартам: Сравнение с ISO/IEC 27017, GDPR	
	2.3.12	Настройка аудита действий пользователей: Логирование и контроль доступа	
Самостоятельная работа при изучении раздела 2 ПМ.03			46
1. Изучение моделей предоставления облачных сервисов (IaaS, PaaS, SaaS) и зон ответственности. 2. Анализ угроз и уязвимостей облачных систем по классификациям CVE и NIST. 3. Обзор международных и российских стандартов безопасности облачных сервисов (ISO/IEC 27017, 27018, ГОСТ Р 57580). 4. Схематическое отображение архитектуры типовой облачной инфраструктуры с указанием уязвимых точек. 5. Изучение механизмов аутентификации и авторизации пользователей (OAuth2, OpenID Connect, SAML). 6. Сравнение методов шифрования данных при передаче и хранении в облаке. 7. Изучение стратегий резервного копирования и восстановления данных (полная, дифференциальная, инкрементальная). 8. Анализ политики безопасности облачного провайдера (AWS, Google Cloud, Yandex Cloud и др.). 9. Изучение принципов сетевой сегментации и схем построения защищённых сетей. 10. Анализ видов межсетевых экранов и их функциональных возможностей. 11. Изучение принципов работы IDS/IPS и их применения в облачных инфраструктурах. 12. Рассмотрение методов защиты от DDoS-атак в облачных сервисах. 13. Исследование технологий резервирования и репликации данных (синхронная, асинхронная). 14. Анализ механизмов обеспечения высокой доступности (High Availability) и балансировки нагрузки. 15. Разработка плана аварийного восстановления облачной инфраструктуры (Disaster Recovery Plan). 16. Изучение инструментов мониторинга и анализа безопасности (ELK, Prometheus, Zabbix, Grafana). 17. Разработка политики ведения, хранения и ротации логов. 18. Изучение моделей управления доступом RBAC и ABAC, примеры политик для ролей. 19. Изучение концепции DevSecOps и методов внедрения безопасности в жизненный цикл ПО. 20. Анализ процессов управления уязвимостями и обновления систем. 21. Разработка схемы реагирования на инциденты информационной безопасности. 22. Создание проекта политики информационной безопасности организации, использующей облачные сервисы. 23. Итоговый отчёт: «Комплекс мер по обеспечению безопасности облачной инфраструктуры предприятия».			
Консультации по разделу 2 ПМ.03			2
Экзамен по разделу 2 ПМ.03			4
Раздел 3. Технологии хранения и анализа данных			150/92
МДК.03.03. Технологии хранения и анализа данных			150/92

Тема 3.1 Инфраструктура и технологии хранения данных	Содержание		20
	1	Введение в технологии хранения данных Классификация хранилищ: DAS, NAS, SAN; роль системного администратора	
	2	NFS и SMB — сетевые файловые протоколы Принцип работы, настройка доступа, разграничение прав, безопасность	
	3	InfiniBand и высокоскоростные интерфейсы Архитектура, преимущества, применение в дата-центрах	
	4	Unified Storage — объединённые хранилища Концепция, примеры реализации, преимущества интеграции NAS/SAN	
	5	Программно-определяемое хранилище (SDS) Принципы SDS, управление через API, CEPH, MinIO	
	6	Гиперконвергентные инфраструктуры Архитектура HCI, сочетание вычислений и хранения, VMware vSAN, Proxmox	
	7	Облачные и эфемерные хранилища Облако как инфраструктура хранения, S3-хранилища, ephemeral volumes	
	8	RAID и избыточность данных RAID 0–10, отказоустойчивость, аппаратная и программная реализация	
	9	Open Source системы хранения CEPH, GlusterFS, TrueNAS, MinIO — обзор и сравнение	
	10	Проприетарные решения Dell EMC, NetApp, VMware vSAN — интеграция в облако	
	Практические занятия		36
	3.1.1	Установка и базовая настройка сервера NFS в Linux: Освоение принципов работы сетевых файловых систем	
	3.1.2	Настройка SMB/CIFS-сервера и подключение клиентов: Изучение технологии совместного доступа к файлам	
	3.1.3	Сравнение производительности NFS и SMB: Анализ эффективности различных протоколов хранения	
	3.1.4	Настройка сетевого хранилища с использованием iSCSI: Ознакомление с блочными протоколами доступа к данным	
	3.1.5	Изучение технологии InfiniBand и её настройки в эмуляторе: Ознакомление с высокоскоростными межсоединениями	
	3.1.6	Развёртывание unified storage на базе Ceph: Практика объединения разных типов хранилищ	
	3.1.7	Настройка программного SDS-хранилища (Software Defined Storage): Изучение программно-определяемых хранилищ	

	3.1.8	Сравнение SDS и традиционных систем хранения: Оценка преимуществ и недостатков SDS	
	3.1.9	Развёртывание гиперконвергентной системы (Proxmox VE или TrueNAS Scale): Изучение принципов объединения хранения и вычислений	
	3.1.10	Настройка RAID-массивов разных уровней (RAID 0/1/5/10): Освоение технологии отказоустойчивого хранения данных	
	3.1.11	Исследование производительности разных уровней RAID: Практический анализ скоростей и надёжности	
	3.1.12	Создание и подключение облачного хранилища (например, MinIO, Nextcloud): Изучение основ организации облачных хранилищ	
	3.1.13	Настройка эфемерных хранилищ в контейнерах: Практика временного хранения данных в облачных средах	
	3.1.14	Мониторинг использования хранилищ (Zabbix, Grafana): Освоение инструментов наблюдения за нагрузкой	
	3.1.15	Настройка политик доступа к данным в сетевом хранилище: Изучение разграничения доступа пользователей	
	3.1.16	Создание сценариев автоматического монтирования хранилищ: Практика автоматизации подключения ресурсов	
	3.1.17	Настройка и тестирование отказоустойчивости хранилища: Проверка работы при сбоях оборудования	
	3.1.18	Итоговый мини-проект: развёртывание корпоративного хранилища: Комплексная интеграция всех изученных технологий	
Тема 3.2 Защита, репликация и миграция данных	Содержание		16
	1	Валидация и контроль целостности данных Проверка хешей, CRC, контроль битовых ошибок	
	2	Хеширование и контроль версий данных MD5, SHA, версионность объектов в S3	
	3	Репликация и резервирование данных LVM snapshot, зеркалирование, георепликация	
	4	Резервное копирование в облаке Инкрементальные, дифференциальные, полные бэкапы	
	5	Миграция данных между средами Перенос данных между хранилищами и облаками (rsync, rclone, AWS CLI)	
	6	Оптимизация и дедупликация данных Алгоритмы сжатия, deduplication, оптимизация дискового пространства	
	7	Контроль доступа и аудита хранения	

		ACL, POSIX-права, IAM-политики, ведение журналов доступа	28
	8	Мониторинг и диагностика систем хранения Zabbix, Prometheus, Grafana, анализ производительности	
	Практические занятия		
	3.2.1	Проверка целостности файлов с помощью контрольных сумм (MD5, SHA256): Изучение хеш-функций и их применения	
	3.2.2	Настройка проверки целостности данных в хранилище (ZFS Scrub, Ceph Health): Контроль целостности в распределённых системах.	
	3.2.3	Настройка автоматического резервного копирования средствами rsync и cron: Освоение базовых средств резервирования	
	3.2.4	Настройка инкрементального резервного копирования (Borg, Duplicity): Повышение эффективности хранения резервов	
	3.2.5	Развёртывание системы централизованного бэкапа (например, Bacula, Veeam): Работа с корпоративными решениями резервирования	
	3.2.6	Тестирование восстановления данных из резервных копий: Проверка работоспособности стратегии бэкапа	
	3.2.7	Настройка шифрования данных на уровне хранилища: Изучение технологий защиты при хранении	
	3.2.8	Настройка VPN-доступа к облачному хранилищу: Практика защиты каналов связи при доступе к данным	
	3.2.9	Настройка политик аудита доступа к данным: Изучение журналирования действий пользователей	
	3.2.10	Разработка плана аварийного восстановления (Disaster Recovery Plan): Формирование стратегии восстановления инфраструктуры	
	3.2.11	Анализ угроз и тестирование защиты облачного хранилища: Отработка навыков безопасности данных	
	3.2.12	Настройка резервирования облака средствами Snapshot: Применение снимков состояния для восстановления	
	3.2.13	Организация геораспределённого резервного копирования: Практика распределения данных по регионам	
3.2.14	Итоговая работа: настройка защищённой системы хранения данных: Комплексное применение средств защиты и бэкапа		
Тема 3.3 Анализ и интеллектуальная обработка данных	Содержание		22
	1	Введение в аналитическую обработку данных Различие OLTP и OLAP, Data Lake, Data Warehouse	
	2	Оперативная аналитическая обработка данных (OLAP)	

		Кубы данных, многомерный анализ, пример ClickHouse	
3		Интеллектуальный анализ данных (Data Mining) Методы классификации, кластеризации, прогнозирования	
4		ETL-процессы и интеграция данных Извлечение, трансформация, загрузка, инструменты (Airbyte, Apache NiFi)	
5		Облачные платформы анализа данных Google BigQuery, AWS Athena, Yandex DataLens	
6		Инструменты визуализации и мониторинга Grafana, Kibana, Metabase	
7		Логирование и анализ событий ELK Stack, Fluentd, Loki	
8		Автоматизация анализа данных Python (pandas, matplotlib), автоматические отчёты	
9		Машинное обучение в инфраструктуре облаков Применение ML для анализа логов и мониторинга	
10		Практика построения дашборда Создание аналитического отчёта по данным системы хранения	
11		Итоговая лекция: Комплексная архитектура хранения и анализа данных Объединение технологий хранения, защиты и анализа	
		Практические занятия	28
3.3.1		Установка и настройка PostgreSQL/MySQL как систем аналитического хранения: Освоение СУБД для хранения и анализа данных	
3.3.2		Импорт и организация структурированных данных: Формирование аналитических наборов данных	
3.3.3		Использование OLAP-кубов и аналитических запросов: Изучение оперативной аналитической обработки	
3.3.4		Настройка инструментов ETL (Extract, Transform, Load): Практика подготовки данных для анализа	
3.3.5		Анализ логов и журналов хранилищ средствами ELK Stack: Освоение инструментов сбора и анализа данных	
3.3.6		Использование Power BI / Metabase для визуализации данных: Развитие навыков представления аналитики	
3.3.7		Настройка мониторинга производительности хранилищ: Анализ метрик и узких мест в инфраструктуре	
3.3.8		Сбор и агрегация данных с разных хранилищ: Интеграция разнородных источников информации	

	3.3.9	Использование Python (pandas) для анализа экспортированных данных: Автоматизация аналитических операций	
	3.3.10	Настройка open-source хранилища данных (Hadoop / ClickHouse / MinIO): Изучение распределённых систем анализа	
	3.3.11	Настройка политики доступа к аналитическим данным: Защита информации при аналитических операциях	
	3.3.12	Сравнение open-source и проприетарных аналитических систем: Анализ преимуществ и ограничений решений	
	3.3.13	Разработка отчётов на основе реальных данных хранилища: Практика построения отчётности	
	3.3.14	Итоговый проект: построение защищённой аналитической платформы: Интеграция хранения, защиты и анализа данных	
Самостоятельная работа при изучении раздела 3 ПМ.03 1. Изучение архитектуры файловых систем Linux и Windows. 2. Анализ принципов работы сетевых хранилищ NAS и SAN. 3. Подготовка отчета о сравнении NFS и SMB по производительности и безопасности. 4. Изучение технологии InfiniBand и ее преимуществ для ЦОД. 5. Обзор концепции Unified Storage и примеров реализации. 6. Изучение архитектуры SDS (Software-Defined Storage). 7. Анализ преимуществ и недостатков гиперконвергентных систем. 8. Подготовка сравнительного анализа облачных и локальных хранилищ. 9. Изучение принципов организации эфемерных хранилищ в облачных платформах. 10. Разработка схемы RAID-массивов различных уровней. 11. Расчет отказоустойчивости для различных конфигураций RAID. 12. Изучение технологий репликации и резервирования данных в облаке. 13. Подготовка отчета о методах миграции данных между облачными платформами. 14. Анализ протоколов передачи данных при миграции больших объемов. 15. Исследование методов валидации данных в распределенных системах. 16. Изучение технологий контроля целостности данных. 17. Выполнение лабораторной работы по хешированию данных. 18. Подготовка обзора современных алгоритмов хеширования. 19. Изучение политики безопасности при хранении конфиденциальных данных. 20. Разработка схемы защиты доступа к файловым хранилищам. 21. Анализ протоколов шифрования данных (TLS, SSL). 22. Изучение инструментов резервного копирования (rsync, Borg, Veeam). 23. Составление плана резервного копирования для локальной сети.			70

24. Подготовка отчета по стратегиям восстановления данных после сбоев. 25. Анализ угроз потери данных при сбое оборудования. 26. Исследование средств мониторинга состояния облачных хранилищ. 27. Настройка систем уведомлений о сбоях и ошибках в хранилищах. 28. Сравнение систем мониторинга Zabbix, Prometheus, Grafana. 29. Подготовка реферата по теме «Роль облачных технологий в инфраструктуре предприятия». 30. Изучение методов оптимизации производительности хранилищ. 31. Исследование влияния сетевых задержек на работу распределенного хранилища. 32. Изучение технологии кэширования данных в облаке. 33. Подготовка отчета об использовании CDN для ускорения доставки данных. 34. Изучение инструментов аналитической обработки данных (OLAP, Power BI, Tableau). 35. Выполнение анализа тестового набора данных средствами SQL. 36. Изучение понятий ETL-процессов и их применения. 37. Подготовка схемы архитектуры хранилища данных (Data Warehouse). 38. Изучение основ интеллектуального анализа данных (Data Mining). 39. Обзор алгоритмов машинного обучения для анализа данных. 40. Изучение инструментов open-source для хранения данных (Nextcloud, Ceph, MinIO). 41. Анализ проприетарных решений хранения данных (Azure Blob, AWS S3, Google Cloud Storage). 42. Сравнение моделей IaaS, PaaS и SaaS в контексте хранения данных. 43. Изучение технологии контейнеризации для организации облачного хранилища. 44. Подготовка отчета о применении Kubernetes для управления хранилищами. 45. Разработка итоговой презентации «Интеграция облачных хранилищ в инфраструктуру предприятия».	
Консультации по разделу 3 ПМ.03	2
Экзамен по разделу 3 ПМ.03	4
Учебная практика Примерный перечень работ: 1. Изучение архитектуры и принципов работы систем виртуализации (VirtualBox, VMware, KVM). 2. Установка и настройка гипервизора типа 1 или 2 на рабочей станции. 3. Создание и конфигурация виртуальных машин с различными ОС (Linux, Windows Server). 4. Настройка виртуальных сетей (NAT, Bridge, Host-only) и обмена данными между виртуальными машинами. 5. Настройка совместного доступа к ресурсам (диски, папки, принтеры) между VM. 6. Создание шаблонов и клонов виртуальных машин для ускорения развертывания. 7. Настройка резервного копирования и восстановления виртуальных машин. 8. Подготовка отчета с описанием структуры виртуальной инфраструктуры и параметров настройки.	108
Производственная практика (по профилю специальности) Примерный перечень работ:	144

1. Анализ существующей IT-инфраструктуры предприятия и выявление возможностей для внедрения виртуализации. 2. Развертывание серверной виртуальной среды (на базе VMware ESXi, Proxmox или KVM). 3. Настройка централизованного управления виртуальными машинами. 4. Автоматизация развертывания сервисов с использованием Docker и docker-compose. 5. Реализация системы мониторинга виртуальной инфраструктуры (Zabbix, Prometheus). 6. Настройка отказоустойчивых решений (кластеризация, балансировка нагрузки). 7. Создание и тестирование скриптов автоматизации рутинных задач (bash, PowerShell, Ansible). 8. Подготовка отчета и презентации с анализом эффективности внедрения виртуализации и автоматизации на предприятии.	
Экзамен квалификационный по модулю	8
Всего	826

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Кабинет информационных технологий:

количество посадочных мест – 25, стол для преподавателя 1 шт., стул для преподавателя 1 шт., компьютерный стол 20 шт., персональный компьютер ПК i3 2120/500Gb/4Gb 20 шт., мультимедийный комплект: проектор, интерактивная доска Elite Panaboard UBT-T880W 1 шт., звуковые колонки 1 шт., доска маркерная меловая комбинированная 1 шт., информационный стенд 2 шт., дидактические пособия.

- ПО: 1. Windows 7(профессиональная лицензия, ООО "Битроникс Владивосток" Контракт № 0320100030814000018-45081 от 09.09.14 № 48609744, №62096196, № 48958910, № 45829305, бессрочно);
2. MS Office 2010 pro (лицензия № 48958910, № 47774898, бессрочно);
3. Autodesk AutoCAD 2019 Edu (свободное);
4. visual c++ 2008 express edition (свободное),
5. oracle vm virtualbox (свободное),
6. cisco packet tracer (свободное),
7. microsoft SQL server 2008 (свободное),
8. k-lite codec pack (свободное),
9. visual studio 2008 (свободное).

Мастерская по компетенции «Облачные технологии»

Персональный компьютер Lenovo ThinkCentreTiny M75 + TiO 24 – 21 шт;

Мультимедийный комплект;

Многофункциональное устройство №2 МФУ Xerox WC3345;

Маршрутизатор №3 MikroTik CCR1016-12G MikroTik.

программное и методическое обеспечение

1. Office Professional Plus 2019 Russian OLV NL Each AcademicEdition Additional Product Microsoft Ireland Operations Limited;
2. Microsoft Windows 10.
3. Oracle vm virtualbox
4. VMware Workstation

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Васильков, А. В. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков, И.А. Васильков. — Москва: ФОРУМ: ИНФРА-М, 2022. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1836631>

2. Симмондс, К. Встраиваемые системы на основе Linux / К. Симмондс; пер. с англ. А.А. Слинкина. - Москва: ДМК Пресс, 2017. - 360 с. - ISBN 978-5-97060-483-0. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1027865>

3.2.2. Электронные издания (электронные ресурсы)

1. Гончаренко, А. Н. Сетевые технологии: учебное пособие / А. Н. Гончаренко. — Москва: МИСИС, 2020. — 92 с. — ISBN 978-5-907227-22-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/178093>

2. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. — 3-е изд., стер. — Москва: ФЛИНТА, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1042499>

3.2.3. Дополнительные источники *(при необходимости)*

1. Аньель, Х. Переход в облако: Практическое руководство по организации облачных вычислений для ученых и IT-специалистов / Х. Аньель, Д. Монтес, Р. Иглесиа Хавьер. - Москва: Альпина ПРО, 2022. - 112 с. - ISBN 978-5-907470-89-7. - Текст: электронный. - URL: <https://znanium.com/catalog/product/2030778>

2. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. — Москва: ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1912987>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Осуществлять развертывание облачной инфраструктуры	Определение профессиональной задачи и этапов ее выполнения	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием. Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам. Защита отчетов по практическим и
ПК 3.2. Проводить документирование требований и технических возможностей облачных инфраструктур	Эффективный поиск информации для решения профессиональной задачи	
ПК 3.3. Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки	Определение ресурсов для решения профессиональной задачи Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует	

ПК 3.4. Производить хранение и анализ данных	техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.	лабораторным работам. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ПК 3.5. Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов	Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен квалификационный
ПК 3.6. Проводить мониторинг системы в облачных сервисах		

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА
для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

МДК.03.01 Технологии виртуализации и автоматизации

программы подготовки специалистов среднего звена

09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2026

Контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине МДК.03.01 Технологии виртуализации и автоматизации разработана в соответствии с требованиями Федерального государственного стандарта среднего профессионального образования по специальности среднего профессионального образования программы подготовки специалистов среднего 09.02.06 Сетевое и системное администрирование, утвержденного приказом Минпросвещения России от 10.07.2023 №519.

Разработчики: Р.С. Реуцкий, преподаватель КСД ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от « 18 » 05 2026 г.

Председатель ЦМК  Е.А. Стефанович
подпись

1 Общие сведения

Контрольно-оценочные средства (далее – КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины МДК.03.01 Технологии виртуализации и автоматизации.

КОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта.

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ПК 3.1	У1	определять общие модели развертывания облачной инфраструктуры
ПК 3.1	У2	определять, насколько данные модели соответствуют требованиям, специфичным для организации
ПК 3.1	У3	пользоваться преимуществами облачной инфраструктуры для снижения операционных нагрузок при развертывании служб
ПК 3.1	У4	проводить оценку, выбирать и внедрять базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище
ПК 3.1	У5	проводить оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности
ПК 3.1	У6	реализовать стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров
ПК 3.1	У7	использовать общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости
ПК 3.2	У8	документировать ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру
ПК 3.2	У9	переводить бизнес-цели и задачи в спецификации, а также презентовать их заинтересованным сторонам
ПК 3.2	У10	создавать внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака
ПК 3.3	У11	проводить оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности
ПК 3.3	У12	анализировать и интерпретировать показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре
ПК 3.3	У13	использовать методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов
ПК 3.3	У14	использовать общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости
ПК 3.1	31	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами
ПК 3.1	32	требования к совместимости компонентов внутри облачной инфраструктуры
ПК 3.1	33	сетевой поток данных и соответствующая зависимость доступности систем

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ПК 3.1, ПК 3.3	34	различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками
ПК 3.1, ПК 3.2	35	как взаимодействовать с бизнес-единицами для определения лучших практик развертывания и создания плана по миграции в облачную инфраструктуру
ПК 3.1	36	важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений
ПК 3.1	37	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами
ПК 3.1, ПК 3.2	38	основные потребности инфраструктурного дизайна для отдельных групп инженеров
ПК 3.1, ПК 3.2	39	различные технологические решения для достижения бизнес-целей
ПК 3.1	310	сетевой поток данных и соответствующая зависимость доступности систем
ПК 3.1	311	важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений
ПК 3.1	312	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами
ПК 3.1	313	требования к совместимости компонентов внутри облачной инфраструктуры
ПК 3.1	314	сетевой поток данных и соответствующая зависимость доступности систем
ПК 3.1	315	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами
ПК 3.1	316	важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений
ПК 3.2	317	методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам
ПК 3.2	318	как взаимодействовать с бизнес-единицами для определения лучших практик развертывания и создания плана по миграции в облачную инфраструктуру
ПК 3.2	319	основные потребности инфраструктурного дизайна для отдельных групп инженеров
ПК 3.2	320	различные технологические решения для достижения бизнес-целей
ПК 3.2	321	методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам
ПК 3.3	322	различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками
ПК 3.3	323	требования к производительности и возможные узкие места при проектировании инфраструктуры
ПК 3.3	324	показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры
ПК 3.3	325	методики и возможности автоматизации, широко используемые в техническом сообществе
ПК 3.3	326	требования к производительности и возможные узкие места при проектировании инфраструктуры

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ПК 3.3	327	различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками
ПК 3.3	328	требования к производительности и возможные узкие места при проектировании инфраструктуры

3 Соответствие оценочных средств контролируемым результатам обучения

3.1 Средства, применяемые для оценки уровня теоретической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
Раздел 1. Технологии виртуализации и автоматизации.				
Тема 1.1 Виртуализация и основы облачных технологий	У1, У2, У3, У4, У5, 31, 32, 33, 34, 35, 36, 37, 38, 39, 310, 311, 312, 313, 314, 315, 316	Объясняет понятие и назначение виртуализации, различает аппаратную и программную виртуализацию, сопоставляет гипервизоры типа 1 и типа 2, характеризует виртуальные ресурсы и виртуальные сети, определяет общие модели развертывания облачной инфраструктуры, определяет, насколько данные модели соответствуют требованиям, специфичным для организации, пользуется преимуществами облачной инфраструктуры для снижения операционных нагрузок при развертывании служб, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности.	Устный опрос (п. 5.1, вопросы 1–10); Реферат (п. 5.2, темы 1–10); Тест №1 (п. 5.3); Тест №2 (п. 5.3)	Экзаменационные билеты №1–6 (п. 6.1)
Тема 1.2 Контейнеризация и оркестрация сервисов	У6, У7, У11, У12, У13, У14, 34, 322, 323, 324, 325, 326, 327, 328	Объясняет отличия контейнеров от виртуальных машин, характеризует архитектуру Docker и Kubernetes, применяет Docker Compose при работе с многоконтейнерными приложениями, реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, проводит оценку, выбор и	Устный опрос (п. 5.1, вопросы 11–21); Реферат (п. 5.2, темы 11–20); Тест №3 (п. 5.3); Тест №4 (п. 5.3)	Экзаменационные билеты №7–17 (п. 6.1)

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
		внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, использует методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов.		
Тема 1.3 Облачные сервисы и безопасность инфраструктуры	У8, У9, У10, 35, 38, 39, 317, 318, 319, 320, 321	Объясняет модели облачных сервисов и облачные бизнес-модели, интерпретирует требования бизнеса к облачной инфраструктуре, документирует ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру, переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, создает внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака, обосновывает различные технологические решения для достижения бизнес-целей, характеризует методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам.	Устный опрос (п. 5.1, вопросы 22–30); Реферат (п. 5.2, темы 21–30); Тест №5 (п. 5.3)	Экзаменационные билеты №18–30 (п. 6.1)

² - для формулировки показателей использовать положения Таксономии Блума.

³ - Однотипные оценочные средства нумеруются, н-р: «Тест №2», «Контрольная работа №4».

⁴ - Примеры всех оценочных средств должны быть представлены в разделах 5,6.

⁵ - В скобках следует указать пункт разделов 5.6, в котором оно представлено.

3.2 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Раздел 1. Технологии виртуализации и автоматизации.				
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 1. Установка и настройка Hosted-гипервизора: Установка VirtualBox или VMware Workstation. Настройка сети NAT и Host-Only.	У1, У4, 31, 32	Выполняет установку и настройку Hosted-гипервизора: Установка VirtualBox или VMware Workstation. Настройка сети NAT и Host-Only, определяет общие модели развертывания облачной инфраструктуры, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, применяет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, учитывает требования к совместимости компонентов внутри облачной инфраструктуры.	Тест №1 (п. 5.3)	Практическое задание экзаменационных билетов № 1–2 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 2. Установка нативного гипервизора: Развёртывание KVM или Proxmox VE на физическом сервере.	У1, У4, 32, 36	Выполняет установку нативного гипервизора: Развёртывание KVM или Proxmox VE на физическом сервере, определяет общие модели развертывания облачной инфраструктуры, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, учитывает требования к совместимости компонентов внутри облачной инфраструктуры, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений.	Тест №1 (п. 5.3)	Практическое задание экзаменационных билетов № 1–4 (п. 6.1)

Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 3. Создание и управление виртуальными машинами: Создание, копирование, клонирование, импорт/экспорт VM.	У3, У4, 36, 311	Выполняет создание и управление виртуальными машинами: Создание, копирование, клонирование, импорт/экспорт VM, пользуется преимуществами облачной инфраструктуры для снижения операционных нагрузок при развертывании служб, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений.	Тест №2 (п. 5.3)	Практическое задание экзаменационных билетов № 2–3 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 4. Настройка виртуальной маршрутизации и сетей: Создание виртуальных мостов, VLAN, NAT, настройка маршрутов.	У4, 31, 33, 310, 312	Выполняет настройку виртуальной маршрутизации и сетей: Создание виртуальных мостов, VLAN, NAT, настройка маршрутов, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, применяет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, учитывает сетевой поток данных и соответствующую зависимость доступности систем.	Тест №3 (п. 5.3)	Практическое задание экзаменационных билетов № 2, № 5 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 5. Автоматизация развёртывания виртуальных машин: Использование шаблонов VM, Cloud-init или Ansible для автоматической настройки.	У3, У4, 35, 38, 39	Выполняет автоматизацию развёртывания виртуальных машин: Использование шаблонов VM, Cloud-init или Ansible для автоматической настройки, пользуется преимуществами облачной инфраструктуры для снижения операционных нагрузок при развертывании служб, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, применяет как взаимодействовать с бизнес-единицами для определения лучших практик развёртывания и создания плана по миграции в облачную инфраструктуру, учитывает основные	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 25–26 (п. 6.1)

		потребности инфраструктурного дизайна для отдельных групп инженеров, соотносит различные технологические решения для достижения бизнес-целей.		
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 6. Конфигурация ресурсов виртуальных машин: Изменение параметров CPU, RAM, дисков, сетей. Управление приоритетами.	У12, У13, 322, 323, 324	Выполняет конфигурацию ресурсов виртуальных машин: Изменение параметров CPU, RAM, дисков, сетей. Управление приоритетами, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, использует методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов, применяет различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры, анализирует показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры.	Тест №4 (п. 5.3)	Практическое задание экзаменационного билета № 13 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем	У3, У4, 33, 314	Выполняет резервное копирование и миграцию виртуальных машин: Создание снимков, восстановление, live migration в Proxmox VE, пользуется преимуществами облачной инфраструктуры для снижения операционных	Тест №3 (п. 5.3)	Практическое задание экзаменационных билетов № 3, № 23 (п. 6.1)

Практическое занятие № 7. Резервное копирование и миграция виртуальных машин: Создание снимков, восстановление, live migration в Proxmox VE.		нагрузок при развертывании служб, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, учитывает сетевой поток данных и соответствующую зависимость доступности систем.		
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 8. Создание отказоустойчивого кластера в Proxmox VE: Настройка двух узлов с репликацией и failover.	У5, 34, 36, 316	Выполняет создание отказоустойчивого кластера в Proxmox VE: Настройка двух узлов с репликацией и failover, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, применяет различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений.	Тест №3 (п. 5.3)	Практическое задание экзаменационных билетов № 4, № 17 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 9. Мониторинг и управление кластером: Использование встроенных инструментов Proxmox для отслеживания состояния VM.	У12, У13, 324, 325	Выполняет мониторинг и управление кластером: Использование встроенных инструментов Proxmox для отслеживания состояния VM, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, использует методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, использует методики и возможности автоматизации, широко используемые в техническом сообществе.	Тест №4 (п. 5.3)	Практическое задание экзаменационных билетов № 22, № 27 (п. 6.1)

Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 10. Развёртывание базовых сервисов внутри VM: Установка LAMP, FTP или DNS-сервера. Проверка сетевой доступности.	У4, 31, 36, 311	Выполняет развёртывание базовых сервисов внутри VM: Установка LAMP, FTP или DNS-сервера. Проверка сетевой доступности, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, применяет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений.	Тест №2 (п. 5.3)	Практическое задание экзаменационного билета № 28 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 11. Развёртывание сервисов конечного пользователя: Настройка HostPanel, базы данных, службы аутентификации.	У4, У8, У10, 35, 317	Выполняет развёртывание сервисов конечного пользователя: Настройка HostPanel, базы данных, службы аутентификации, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, документирует ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру, создает внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака, применяет методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам.	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 20, № 29 (п. 6.1)
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 12. Создание изолированной виртуальной сети: Настройка внутренней сети для	У4, 31, 33, 312	Выполняет создание изолированной виртуальной сети: Настройка внутренней сети для тестирования сервисов, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, применяет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, учитывает сетевой поток данных и соответствующую зависимость	Тест №3 (п. 5.3)	Практическое задание экзаменационных билетов № 5, № 21 (п. 6.1)

тестирования сервисов.		доступности систем.		
Тема 1.1 Виды и содержание типовых инструкций по эксплуатации, обслуживанию и ремонту инфокоммуникационных систем Практическое занятие № 13. Мини-проект: виртуализированная инфраструктура кампуса: Студент моделирует схему сети из нескольких VM и настраивает взаимодействие между ними.	У1, У4, У5, У12, 31, 33, 34, 324	Выполняет мини-проект: виртуализированная инфраструктура кампуса: Студент моделирует схему сети из нескольких VM и настраивает взаимодействие между ними, определяет общие модели развертывания облачной инфраструктуры, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуры.	Тест №5 (п. 5.3)	Практическое задание экзаменационного билета № 30 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 1. Введение в Docker и контейнеризацию: Установка Docker Engine, создание первого контейнера.	У6, 34	Выполняет введение в Docker и контейнеризацию: Установка Docker Engine, создание первого контейнера, реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, применяет различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками.	Тест №1 (п. 5.3)	Практическое задание экзаменационного билета № 7 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 2. Работа с образами Docker: Создание собственного Dockerfile, публикация образа.	У6, 39	Выполняет работу с образами Docker: Создание собственного Dockerfile, публикация образа, реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, соотносит различные технологические решения для достижения бизнес-целей.	Тест №2 (п. 5.3)	Практическое задание экзаменационного билета № 8 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов	У6, У7, 31, 33	Выполняет управление контейнерами и томами: Подключение томов, монтирование данных,	Тест №2 (п. 5.3)	Практическое задание

Практическое занятие № 3. Управление контейнерами и томами: Подключение томов, монтирование данных, настройка сетей контейнеров.		настройка сетей контейнеров, реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, применяет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, учитывает сетевой поток данных и соответствующую зависимость доступности систем.		экзаменационных билетов № 8–9 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 4. Многоконтейнерные приложения с Docker Compose: Развёртывание web-приложения (Nginx + PHP + DB).	У6, У7, 36, 311	Выполняет многоконтейнерные приложения с Docker Compose: Развёртывание web-приложения (Nginx + PHP + DB), реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений.	Тест №1 (п. 5.3)	Практическое задание экзаменационного билета № 9 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 5. Установка Kubernetes в среде Proxmox VE: Создание кластера Kubernetes на 2–3 узлах.	У6, У11, 322, 323	Выполняет установку Kubernetes в среде Proxmox VE: Создание кластера Kubernetes на 2–3 узлах, реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, применяет различные варианты производительности инфраструктуры, доступные благодаря таким	Тест №3 (п. 5.3)	Практическое задание экзаменационного билета № 10 (п. 6.1)

		решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры.		
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 6. Настройка Kubernetes и деплой приложения: Развёртывание подов, сервисов и ingress.	У7, У11, У14, 324, 325	Выполняет настройку Kubernetes и деплой приложения: Развёртывание подов, сервисов и ingress, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, использует методики и возможности автоматизации, широко используемые в техническом сообществе.	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 10–12 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 7. Оркестрация контейнеров Kubernetes: Репликация, масштабирование и автообновления приложений.	У11, У12, У14, 322, 324, 326	Выполняет оркестрацию контейнеров Kubernetes: Репликация, масштабирование и автообновления приложений, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, применяет различные варианты производительности	Тест №4 (п. 5.3)	Практическое задание экзаменационных билетов № 11–12 (п. 6.1)

		инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками.		
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 8. Работа с kubectl: Основные команды, получение статуса узлов и подов.	У12, У13, 324, 325	Выполняет работу с kubectl: Основные команды, получение статуса узлов и подов, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуры, использует методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, использует методики и возможности автоматизации, широко используемые в техническом сообществе.	Тест №3 (п. 5.3)	Практическое задание экзаменационного билета № 13 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 9. Мониторинг и логирование контейнеров: Настройка Fluent Bit, Prometheus или встроенного log-доступа.	У12, У13, 324, 325	Выполняет мониторинг и логирование контейнеров: Настройка Fluent Bit, Prometheus или встроенного log-доступа, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуры, использует методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, использует методики и возможности автоматизации, широко используемые в техническом сообществе.	Тест №4 (п. 5.3)	Практическое задание экзаменационных билетов № 14, № 22 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 10. Настройка отказоустойчивости и	У11, У14, 322, 324, 327	Выполняет настройку отказоустойчивости и балансировки: Создание LoadBalancer и NodePort сервисов, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы	Тест №5 (п. 5.3)	Практическое задание экзаменационного билета № 17 (п. 6.1)

балансировки: Создание LoadBalancer и NodePort сервисов.		управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, применяет различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками.		
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 11. Сетевые политики и безопасность подов: Настройка NetworkPolicy для ограничения трафика.	У14, 323, 324	Выполняет сетевые политики и безопасность подов: Настройка NetworkPolicy для ограничения трафика, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры.	Тест №4 (п. 5.3)	Практическое задание экзаменационных билетов № 16, № 21 (п. 6.1)
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 12. Резервное копирование и восстановление контейнеров: Работа с Velero, сохранение состояния и восстановление приложения.	У14, 324, 328	Выполняет резервное копирование и восстановление контейнеров: Работа с Velero, сохранение состояния и восстановление приложения, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, использует общедоступные облачные службы и функции для поддержки разработки и внедрения	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 15, № 23 (п. 6.1)

		решений в соответствии с требованиями доступности, надежности и масштабируемости, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры.		
Тема 1.2. Контейнеризация и оркестрация сервисов Практическое занятие № 13. Мини-проект: кластерная среда для корпоративного портала: Развёртывание корпоративного портала в Kubernetes с балансировкой и логированием.	У6, У7, У11, У12, У14, 322, 324, 325, 327	Выполняет мини-проект: кластерная среда для корпоративного портала: Развёртывание корпоративного портала в Kubernetes с балансировкой и логированием, реализует стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре.	Тест №5 (п. 5.3)	Практическое задание экзаменационного билета № 30 (п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 1 Введение в облачные бизнес-модели (IaaS, PaaS, SaaS): Работа с примерами публичных облаков (AWS, Yandex Cloud).	У9, 318, 320	Выполняет введение в облачные бизнес-модели (IaaS, PaaS, SaaS): Работа с примерами публичных облаков (AWS, Yandex Cloud), переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, применяет как взаимодействовать с бизнес-единицами для определения лучших практик развертывания и создания плана по миграции в облачную инфраструктуру, соотносит различные технологические решения для достижения бизнес-	Тест №1 (п. 5.3)	Практическое задание экзаменационных билетов № 18–19 (п. 6.1)

		целей.		
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 2 Развёртывание IaaS в локальной среде: Настройка виртуальной инфраструктуры как услуги в Proxmox/OpenStack.	У4, У8, У9, 35, 39	Выполняет развёртывание IaaS в локальной среде: Настройка виртуальной инфраструктуры как услуги в Proxmox/OpenStack, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, документирует ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру, переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, применяет как взаимодействовать с бизнес-единицами для определения лучших практик развертывания и создания плана по миграции в облачную инфраструктуру, соотносит различные технологические решения для достижения бизнес-целей.	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 18, № 26 (п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 3 Автоматизация IaaS-развёртывания: Использование Terraform или Ansible для создания VM по шаблону.	У4, У9, У10, 318, 319, 320	Выполняет автоматизацию IaaS-развёртывания: Использование Terraform или Ansible для создания VM по шаблону, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, создает внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака, применяет основные потребности инфраструктурного дизайна для отдельных групп инженеров, соотносит различные технологические решения для достижения бизнес-целей.	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 25–26 (п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 4 Балансировщик нагрузки	У5, У11, У12, 34, 322, 324	Выполняет балансировщик нагрузки виртуальных машин: Настройка HAProxy или Nginx Load Balancer, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы	Тест №4 (п. 5.3)	Практическое задание экзаменационных билетов № 17, № 19

виртуальных машин: Настройка HAProxy или Nginx Load Balancer.		управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, применяет различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры.		(п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 5 PaaS: настройка платформы для web-приложений: Развёртывание контейнерного PaaS (например, Dokku, Portainer).	У7, У9, 39, 320	Выполняет PaaS: настройка платформы для web-приложений: Развёртывание контейнерного PaaS (например, Dokku, Portainer), использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, соотносит различные технологические решения для достижения бизнес-целей.	Тест №1 (п. 5.3)	Практическое задание экзаменационного билета № 18 (п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 6 SaaS: настройка облачного приложения: Развёртывание Nextcloud, мониторинг, резервирование данных.	У7, У12, 324, 327	Выполняет SaaS: настройка облачного приложения: Развёртывание Nextcloud, мониторинг, резервирование данных, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, применяет показатели системы,	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 19, № 23 (п. 6.1)

		сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, применяет различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками.		
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 7 Контроль доступа и авторизация в облачной инфраструктуре: Создание ролей, управление ключами, политика доступа.	У10, 317, 321	Выполняет контроль доступа и авторизация в облачной инфраструктуре: Создание ролей, управление ключами, политика доступа, создает внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака, применяет методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам.	Тест №5 (п. 5.3)	Практическое задание экзаменационных билетов № 20, № 29 (п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры Практическое занятие № 8 Мониторинг и аудит событий безопасности: Анализ логов, настройка оповещений, журналирование.	У9, У12, 317, 324, 325	Выполняет мониторинг и аудит событий безопасности: Анализ логов, настройка оповещений, журналирование, переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре, применяет методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам, применяет показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры, использует методики и возможности автоматизации, широко используемые в техническом сообществе.	Тест №5 (п. 5.3)	Практическое задание экзаменационного билета № 22 (п. 6.1)
Тема 1.3 Облачные сервисы и безопасность инфраструктуры	У4, У7, У8, У9, У10,	Выполняет финальный мини-проект: безопасная облачная инфраструктура организации: Проект	Тест №5 (п. 5.3)	Практическое задание

Практическое занятие № 9 Финальный мини-проект: безопасная облачная инфраструктура организации: Проект объединяет виртуализацию, контейнеризацию и безопасность в единой системе.	У11, У12, У14, 35, 39, 317, 320, 324, 325	объединяет виртуализацию, контейнеризацию и безопасность в единой системе, проводит оценку, выбирает и внедряет базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, документирует ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру, переводит бизнес-цели и задачи в спецификации, а также презентует их заинтересованным сторонам, создает внутренние руководящие документы и требования к процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака, проводит оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности, анализирует и интерпретирует показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре.		экзаменационного билета № 30 (п. 6.1)
--	--	--	--	--

4 Описание процедуры оценивания

Результаты обучения по дисциплине, уровень сформированности компетенций оцениваются по четырём бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом.

Критерии оценивания устного ответа

Оценочные средства: собеседование, устное сообщение

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

Оценочные средства: доклад (сообщение), в том числе выполненный в форме презентации.

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера.

Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	<i>Отлично</i>	<i>Хорошо</i>	<i>Удовлетворительно</i>	<i>Неудовлетворительно</i>
Количество правильных ответов	91 % и $\geq$	от 81% до 90,9 %	не менее 70%	менее 70%

Критерии выставления оценки студенту на зачете/ экзамене

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только

	основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

1. Что такое виртуализация и для чего она используется в ИТ-инфраструктуре?
2. Чем отличается аппаратная виртуализация от программной виртуализации?
3. В чем различие между гипервизорами типа 1 и типа 2?
4. Какие возможности предоставляют виртуальные процессоры, память, диски и сетевые адаптеры в виртуальной машине?
5. Что такое виртуальный коммутатор, и какую роль он играет в работе виртуальной сети?
6. Чем отличаются режимы NAT, Bridge и Host-Only при настройке сети виртуальных машин?
7. Для чего используются снимки виртуальных машин, клонирование и миграция?
8. Что такое кластеризация в виртуальной инфраструктуре и зачем она нужна?
9. В чем заключается отказоустойчивость виртуальной инфраструктуры?
10. Как виртуализация связана с облачными технологиями?
11. Что такое контейнеризация и чем контейнер отличается от виртуальной машины?
12. Какие основные компоненты входят в архитектуру Docker?
13. Для чего нужен Dockerfile и что обычно в нем описывается?
14. Для чего используется Docker Compose при работе с многоконтейнерными приложениями?
15. Что такое Kubernetes и для каких задач он применяется?
16. Что такое pod, deployment и service в Kubernetes?
17. Для чего в Kubernetes используются ConfigMap и Secret?
18. Что понимается под масштабированием приложения в Kubernetes?
19. Какую роль играет планировщик Kubernetes при распределении ресурсов?
20. Для чего нужны логирование и мониторинг в контейнерной среде?
21. Какие способы резервного копирования и восстановления можно применять для контейнеров и контейнерных сервисов?
22. Что означают модели облачных сервисов IaaS, PaaS и SaaS?
23. Чем отличаются IaaS, PaaS и SaaS друг от друга на практическом уровне?
24. Что понимается под облачными бизнес-моделями и гибкой моделью оплаты облачных услуг?
25. Какие меры применяются для обеспечения безопасности виртуальной инфраструктуры?
26. Что включает в себя сетевая безопасность в облачной инфраструктуре?
27. Для чего нужен мониторинг и аудит в облачной инфраструктуре?
28. Что такое Disaster Recovery и почему эта стратегия важна для облачных сервисов?

29. Какие средства можно использовать для автоматизации развертывания облачной или виртуальной инфраструктуры?
30. В чем заключается практическая интеграция виртуализации, контейнеризации и средств безопасности в единой инфраструктуре?

5.2 Темы рефератов

1. Виртуализация как основа современной ИТ-инфраструктуры
2. Аппаратная и программная виртуализация: принципы, различия, применение
3. Гипервизоры типа 1 и типа 2: сравнительный анализ
4. Организация виртуальных ресурсов в современной вычислительной среде
5. Виртуальные сети и коммутация в инфраструктуре виртуальных машин
6. Инструменты виртуализации QEMU, KVM и Virt-manager: возможности и особенности
7. Proxmox VE как платформа для построения виртуализированной инфраструктуры
8. Кластеризация и отказоустойчивость в виртуальной среде
9. Роль виртуализации в развитии облачных технологий
10. Облачные платформы OpenStack, Proxmox и VMware Cloud: обзор и сравнение
11. Контейнеризация как этап развития виртуализации
12. Контейнеры и виртуальные машины: отличия, преимущества и ограничения
13. Архитектура Docker и ее роль в развертывании приложений
14. Docker Compose как средство развертывания многоконтейнерных приложений
15. Kubernetes как платформа оркестрации контейнеров
16. Основные компоненты Kubernetes и их назначение
17. Масштабирование и обновление приложений в Kubernetes
18. Планирование и распределение ресурсов в Kubernetes-кластере
19. Логирование и мониторинг в контейнерной инфраструктуре
20. Резервное копирование и восстановление контейнеризированных приложений
21. Модели облачных сервисов IaaS, PaaS, SaaS: особенности и примеры
22. Облачные бизнес-модели и экономические преимущества облачных решений
23. Безопасность виртуальной инфраструктуры: принципы и инструменты
24. Контроль доступа и защита API в облачной инфраструктуре
25. Сетевая безопасность в облаках: VPN, firewall, сегментация и политики безопасности
26. Мониторинг, аудит и журналирование событий в облачной инфраструктуре
27. Disaster Recovery как элемент обеспечения устойчивости облачных сервисов
28. Автоматизация развертывания облачной инфраструктуры с помощью Terraform и Ansible
29. Интеграция контейнеризации, виртуализации и средств безопасности в единой инфраструктуре
30. Перспективы развития облачных технологий и инфраструктурных сервисов

5.3 Примеры тестовых заданий

Тест №1

1. Что такое виртуализация?
 - а) Способ резервного копирования данных
 - б) Технология создания виртуальных ресурсов на базе физического оборудования (верно)
 - в) Метод шифрования файлов
 - г) Средство мониторинга сетевого трафика
2. Какой гипервизор относится к типу 1?
 - а) VirtualBox
 - б) VMware Workstation

- в) VMware ESXi (верно)
- г) Docker Desktop

3. Что позволяет режим NAT при настройке сети виртуальной машины?

- а) Только обмен файлами между двумя VM
- б) Доступ виртуальной машины во внешнюю сеть через хост (верно)
- в) Полное отключение сети
- г) Только локальную печать

4. Для чего используется snapshot виртуальной машины?

- а) Для сохранения состояния виртуальной машины на определенный момент времени (верно)
- б) Для установки драйверов
- в) Для физической замены диска
- г) Для удаления операционной системы

5. Что является основным отличием контейнера от виртуальной машины?

- а) Контейнер всегда медленнее виртуальной машины
- б) Контейнер использует ядро хостовой операционной системы (верно)
- в) Контейнеру обязательно нужен BIOS
- г) Контейнер не может работать с сетью

6. Что такое Docker Image?

- а) Физический сервер
- б) Файл подкачки Linux
- в) Шаблон для создания контейнеров (верно)
- г) Отдельный pod в Kubernetes

7. Для чего используется Docker Compose?

- а) Для управления многоконтейнерными приложениями (верно)
- б) Для настройки маршрутизатора
- в) Для диагностики дисков
- г) Для шифрования контейнеров

8. Что такое pod в Kubernetes?

- а) Виртуальный коммутатор
- б) Единица развертывания, содержащая один или несколько контейнеров (верно)
- в) Сетевой драйвер Windows
- г) Архив с логами

9. Что обозначает модель IaaS?

- а) Готовое программное обеспечение как услуга
- б) Инфраструктура как услуга (верно)
- в) Платформа для разработки игр
- г) Сервис резервного копирования

10. Для чего нужен мониторинг инфраструктуры?

- а) Только для оформления документации
- б) Для отслеживания состояния систем и выявления сбоев (верно)
- в) Только для удаления журналов
- г) Для замены антивируса

Время выполнения – 10 минут

Тест №2

1. Что относится к виртуальным ресурсам?
 - а) Виртуальные процессоры, память, диски, сетевые адаптеры (верно)
 - б) Только монитор и клавиатура
 - в) Только интернет-кабель
 - г) Только BIOS и UEFI

2. Что такое гипервизор типа 2?
 - а) Гипервизор, работающий поверх операционной системы (верно)
 - б) Гипервизор, встроенный в маршрутизатор
 - в) Гипервизор, который работает только в облаке
 - г) Средство контейнеризации

3. Для чего используется виртуальный коммутатор?
 - а) Для подключения виртуальных машин к сети (верно)
 - б) Для архивации образов
 - в) Для удаления снапшотов
 - г) Для установки Kubernetes

4. Что позволяет клонирование виртуальной машины?
 - а) Удалить сетевую карту
 - б) Создать копию виртуальной машины (верно)
 - в) Увеличить частоту процессора
 - г) Сжать оперативную память

5. Что такое Docker Container?
 - а) Запущенный экземпляр образа (верно)
 - б) Файл конфигурации сети
 - в) Физический сервер
 - г) Тип гипервизора

6. Для чего нужен Dockerfile?
 - а) Для описания шагов создания Docker-образа (верно)
 - б) Для настройки BIOS
 - в) Для резервного копирования диска
 - г) Для обновления ядра хоста

7. Что такое Deployment в Kubernetes?
 - а) Служба хранения данных
 - б) Объект для управления развертыванием и обновлением приложений (верно)
 - в) Команда Linux для проверки сети
 - г) Тип виртуального диска

8. Что делает ReplicaSet в Kubernetes?
 - а) Следит за количеством экземпляров pod (верно)
 - б) Удаляет все контейнеры
 - в) Управляет BIOS виртуальной машины
 - г) Настраивает VPN

9. Что означает модель SaaS?
- а) Сервер как система
 - б) Безопасность как услуга
 - в) Программное обеспечение как услуга (верно)
 - г) Хранилище как сеть

10. Что включает в себя Disaster Recovery?
- а) Только обновление интерфейса
 - б) Только очистку логов
 - в) Восстановление сервисов после сбоев (верно)
 - г) Сжатие образов контейнеров

Время выполнения – 10 минут

Тест №3

1. Что такое кластеризация в виртуальной инфраструктуре?
- а) Объединение ресурсов нескольких узлов для повышения отказоустойчивости и управления (верно)
 - б) Удаление неиспользуемых контейнеров
 - в) Шифрование базы данных
 - г) Установка одной VM на один сервер
2. Для чего используется VLAN в виртуальной среде?
- а) Для логического разделения сетевого трафика (верно)
 - б) Для увеличения объема диска
 - в) Для замены гипервизора
 - г) Для резервного копирования памяти
3. Что такое live migration?
- а) Перенос виртуальной машины между узлами без значительной остановки (верно)
 - б) Удаление виртуальной машины
 - в) Установка новой ОС
 - г) Переключение сети NAT в Bridge
4. Какое преимущество дает контейнеризация?
- а) Более быстрый запуск приложений и эффективное использование ресурсов (верно)
 - б) Полный отказ от сети
 - в) Замена всех баз данных
 - г) Уменьшение объема оперативной памяти до нуля
5. Что хранится в Registry Docker?
- а) Образы контейнеров (верно)
 - б) Таблицы маршрутизации
 - в) Запущенные pod
 - г) Сетевые ключи Wi-Fi
6. Для чего нужен kubectl?
- а) Для управления кластером Kubernetes (верно)
 - б) Для сборки ядра Linux
 - в) Для создания BIOS

г) Для настройки принтера

7. Что такое ConfigMap в Kubernetes?

- а) Объект для хранения неконфиденциальных параметров конфигурации (верно)
- б) Средство антивирусной защиты
- в) Тип контейнерного образа
- г) Программа для резервного копирования

8. Что такое Secret в Kubernetes?

- а) Средство виртуализации
- б) Объект для хранения конфиденциальных данных (верно)
- в) Физический сервер
- г) Команда Docker Compose

9. Что относится к PaaS?

- а) Готовая виртуальная машина с полным управлением железом
- б) Платформа для разработки и развертывания приложений (верно)
- в) Офисный пакет по подписке
- г) Резервное копирование локального диска

10. Для чего применяется аудит в облачной инфраструктуре?

- а) Для отслеживания событий и действий в системе (верно)
- б) Для замены контейнеров на виртуальные машины
- в) Для уменьшения размера монитора
- г) Для отключения маршрутизации

Время выполнения – 10 минут

Тест №4

1. Что такое KVM?

- а) Средство аппаратной виртуализации в Linux (верно)
- б) Система управления печатью
- в) Протокол резервного копирования
- г) Текстовый редактор

2. Для чего используется Proxmox VE?

- а) Для управления виртуальными машинами и контейнерами (верно)
- б) Для создания электронных таблиц
- в) Для настройки веб-дизайна
- г) Для шифрования PDF

3. Что делает режим Host-Only?

- а) Обеспечивает связь VM только с хостом и другими VM этой сети (верно)
- б) Дает прямой выход в интернет без хоста
- в) Полностью удаляет сетевой интерфейс
- г) Используется только в Kubernetes

4. Что такое Docker Engine?

- а) Среда выполнения контейнеров Docker (верно)
- б) Антивирус для Linux
- в) Гипервизор типа 1

г) Компонент BIOS

5. Что описывается в файле docker-compose.yml?

- а) Несколько сервисов, сети и тома приложения (верно)
- б) Только настройки мыши
- в) Только физические диски
- г) Только правила firewall Windows

6. Что такое Service в Kubernetes?

- а) Объект для обеспечения доступа к pod и сетевого взаимодействия (верно)
- б) Тип гипервизора
- в) Системный журнал Linux
- г) Метод клонирования VM

7. Для чего используется масштабирование в Kubernetes?

- а) Для увеличения количества экземпляров приложения при необходимости (верно)
- б) Для отключения контейнеров
- в) Для создания виртуального BIOS
- г) Для удаления журналов

8. Что такое QoS в Kubernetes?

- а) Механизм классификации ресурсов и приоритетов для pod (верно)
- б) Способ удаления контейнеров
- в) Тип SaaS-приложения
- г) Формат резервной копии

9. Что относится к средствам сетевой безопасности в облаке?

- а) VPN, firewall, сегментация сети (верно)
- б) Только текстовый редактор
- в) Только офисный пакет
- г) Только резервное копирование образов

10. Для чего нужна сегментация сети?

- а) Для разделения трафика и повышения безопасности (верно)
- б) Для увеличения размера диска
- в) Для отключения журналирования
- г) Для удаления пользователей

Время выполнения – 10 минут

Тест №5

1. Что означает переход от виртуализации к облачным технологиям?

- а) Отказ от сети в инфраструктуре
- б) Использование виртуализированных ресурсов как сервисов с гибким управлением (верно)
- в) Замену всех серверов ноутбуками
- г) Полный отказ от автоматизации

2. Что такое балансировка нагрузки?

- а) Распределение запросов и нагрузки между ресурсами (верно)
- б) Удаление лишних контейнеров

- в) Выключение резервных серверов
- г) Создание только одной виртуальной машины

3. Для чего применяется Ansible или Terraform в инфраструктуре?

- а) Для автоматизации развертывания и настройки ресурсов (верно)
- б) Для ручного ремонта оборудования
- в) Для замены Kubernetes на BIOS
- г) Для отключения логирования

4. Что такое ingress в Kubernetes?

- а) Механизм управления внешним доступом к сервисам кластера (верно)
- б) Тип виртуального процессора
- в) Формат контейнерного образа
- г) Метод клонирования диска

5. Для чего используется NetworkPolicy в Kubernetes?

- а) Для ограничения и управления сетевым трафиком между pod (верно)
- б) Для увеличения памяти VM
- в) Для удаления Deployment
- г) Для резервного копирования Dockerfile

6. Что дает резервное копирование в инфраструктуре?

- а) Возможность восстановления данных и сервисов (верно)
- б) Только увеличение скорости процессора
- в) Только очистку логов
- г) Только создание новых пользователей

7. Что такое журналирование?

- а) Процесс записи событий системы и приложений (верно)
- б) Удаление контейнеров
- в) Установка новой ОС
- г) Настройка монитора

8. Что включает защита API в облачной инфраструктуре?

- а) Контроль доступа, аутентификацию и ограничение обращений (верно)
- б) Только замену кабелей
- в) Только форматирование дисков
- г) Только настройку принтера

9. Что является примером SaaS-решения?

- а) Nextcloud как готовое облачное приложение для пользователя (верно)
- б) KVM
- в) VLAN
- г) kubelet

10. Что означает отказоустойчивость инфраструктуры?

- а) Способность системы продолжать работу при сбоях отдельных компонентов (верно)
- б) Полное отключение резервирования
- в) Запрет на использование контейнеров
- г) Работа только на одном сервере

Время выполнения – 10 минут

6. Примеры оценочных средств для проведения промежуточной аттестации

6.1 Варианты экзаменационных билетов:

Экзаменационный билет №1

1. Понятие и назначение виртуализации. Аппаратная и программная виртуализация.
2. Гипервизоры типа 1 и типа 2. Сравнительный анализ.

Практическое задание:

Установить и настроить Hosted-гипервизор. Создать виртуальную машину и настроить для нее сеть NAT.

Экзаменационный билет №2

1. Виртуальные ресурсы: виртуальные процессоры, память, диски, сетевые адаптеры.
2. Виртуальная сеть и коммутация: сетевые мосты, виртуальные коммутаторы, NAT.

Практическое задание:

Создать виртуальную машину, настроить виртуальный сетевой адаптер и организовать связь между двумя виртуальными машинами.

Экзаменационный билет №3

1. Инструменты виртуализации QEMU, KVM, Virt-manager.
2. Создание и управление виртуальными машинами, снимки, клонирование, миграции.

Практическое задание:

Создать виртуальную машину, выполнить ее клонирование и создать снимок состояния.

Экзаменационный билет №4

1. Кластеризация и отказоустойчивость в виртуальной инфраструктуре.
2. Обзор Proxmox VE и его возможности.

Практическое задание:

Настроить два узла виртуальной инфраструктуры и описать схему отказоустойчивого кластера.

Экзаменационный билет №5

1. Интеграция виртуализации и сетевого администрирования.
2. VLAN, маршрутизация и управление доступом в виртуальной среде.

Практическое задание:

Настроить изолированную виртуальную сеть для группы виртуальных машин.

Экзаменационный билет №6

1. Введение в понятие облака.
2. Переход от виртуализации к облачным технологиям.

Практическое задание:

Смоделировать схему облачной инфраструктуры на базе виртуальных машин и описать ее основные компоненты.

Экзаменационный билет №7

1. Контейнеризация как развитие виртуализации.
2. Отличия контейнеров от виртуальных машин.

Практическое задание:

Установить Docker Engine и создать первый контейнер.

Экзаменационный билет №8

1. Архитектура Docker: Docker Engine, Registry, Image, Container.
2. Управление образами и контейнерами.

Практическое задание:

Создать собственный Dockerfile и собрать образ контейнера.

Экзаменационный билет №9

1. Docker Compose и многоконтейнерные приложения.
2. Файлы docker-compose.yml, настройка сетей, томов и сервисов.

Практическое задание:

Развернуть многоконтейнерное приложение с использованием Docker Compose.

Экзаменационный билет №10

1. Основы Kubernetes: master, node, pod, service.
2. Назначение etcd, kubelet, kube-proxy.

Практическое задание:

Развернуть pod и service в Kubernetes и проверить их работоспособность.

Экзаменационный билет №11

1. Управление приложениями в Kubernetes.
2. Deployment, ReplicaSet, ConfigMap, Secret.

Практическое задание:

Создать Deployment и выполнить масштабирование приложения.

Экзаменационный билет №12

1. Принципы масштабирования и обновления приложений в Kubernetes.
2. Репликация и управление доступностью сервисов.

Практическое задание:

Настроить обновление контейнерного приложения и увеличить количество реплик.

Экзаменационный билет №13

1. Планирование и распределение ресурсов в Kubernetes.
2. Планировщик, приоритизация, вытеснение, QoS.

Практическое задание:

Проанализировать распределение ресурсов в кластере Kubernetes и предложить способ оптимизации.

Экзаменационный билет №14

1. Сбор логов и мониторинг в Kubernetes.
2. Архитектура сбора логов на уровне узлов и кластера.

Практическое задание:

Настроить просмотр логов контейнера и выполнить базовый мониторинг состояния pod.

Экзаменационный билет №15

1. Резервное копирование и миграции контейнеров.
2. Восстановление и перенос сервисов между узлами и кластерами.

Практическое задание:

Выполнить резервное копирование контейнеризированного приложения и описать порядок его восстановления.

Экзаменационный билет №16

1. Сетевые политики и безопасность pod в Kubernetes.
2. Ограничение трафика и безопасность контейнерной среды.

Практическое задание:

Настроить NetworkPolicy для ограничения сетевого взаимодействия между pod.

Экзаменационный билет №17

1. Отказоустойчивость и балансировка в контейнерной инфраструктуре.
2. LoadBalancer и NodePort сервисы.

Практическое задание:

Настроить доступ к приложению через NodePort или LoadBalancer.

Экзаменационный билет №18

1. Модели облачных сервисов IaaS, PaaS, SaaS.
2. Принципы, различия и примеры реализации.

Практическое задание:

Определить, к какой модели относится заданный облачный сервис, и обосновать ответ.

Экзаменационный билет №19

1. Облачные бизнес-модели.
2. Экономика облачных решений и гибкие модели оплаты.

Практическое задание:

Сравнить использование локальной инфраструктуры и облачного решения для организации.

Экзаменационный билет №20

1. Безопасность виртуальной инфраструктуры.
2. Изоляция пользователей, контроль доступа, разграничение прав, защита API.

Практическое задание:

Настроить роли доступа для пользователей в облачной или виртуальной инфраструктуре.

Экзаменационный билет №21

1. Сетевая безопасность в облаках.
2. Безопасная маршрутизация, VPN, firewall, сегментация и политики безопасности.

Практическое задание:

Разработать схему защищенной сетевой инфраструктуры с использованием firewall и сегментации.

Экзаменационный билет №22

1. Мониторинг и аудит в облачной инфраструктуре.
2. Журналирование, анализ логов, реагирование на инциденты.

Практическое задание:

Настроить сбор журналов и предложить порядок реагирования на инцидент.

Экзаменационный билет №23

1. Резервирование и восстановление после сбоев.
2. Стратегии Disaster Recovery.

Практическое задание:

Разработать план резервного копирования и восстановления для облачного сервиса.

Экзаменационный билет №24

1. Практическая интеграция безопасности и оркестрации.
2. Обеспечение безопасности контейнеров и виртуальных машин в единой инфраструктуре.

Практическое задание:

Предложить меры защиты для инфраструктуры, включающей виртуальные машины и контейнеры.

Экзаменационный билет №25

1. Автоматизация развёртывания виртуальных машин.
2. Использование шаблонов VM, Cloud-init или Ansible для автоматической настройки.

Практическое задание:

Подготовить шаблон виртуальной машины и описать порядок автоматического развёртывания.

Экзаменационный билет №26

1. Автоматизация IaaS-развёртывания.
2. Использование Terraform или Ansible для создания VM по шаблону.

Практическое задание:

Составить пример последовательности действий для автоматизированного развёртывания виртуальной машины.

Экзаменационный билет №27

1. Мониторинг и управление кластером виртуальных машин.
2. Использование встроенных инструментов Proxmox для отслеживания состояния VM.

Практическое задание:

Выполнить проверку состояния виртуальных машин и определить возможные причины сбоя одной из них.

Экзаменационный билет №28

1. Развёртывание базовых сервисов внутри виртуальных машин.
2. Сетевая доступность сервисов LAMP, FTP или DNS.

Практическое задание:

Развернуть один базовый сервис внутри виртуальной машины и проверить его сетевую доступность.

Экзаменационный билет №29

1. Контроль доступа и авторизация в облачной инфраструктуре.
2. Создание ролей, управление ключами, политика доступа.

Практическое задание:

Настроить пользователя, роль и права доступа к ресурсу в облачной инфраструктуре.

Экзаменационный билет №30

1. Интеграция виртуализации, контейнеризации и облачной безопасности в единой системе.
2. Принципы построения современной облачной инфраструктуры организации.

Практическое задание:

Разработать схему инфраструктуры организации, включающую виртуальные машины, контейнеры, мониторинг и меры безопасности.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА
для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

МДК.03.02 Безопасность облачных сервисов

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2025

Контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине МДК.03.02 Безопасность облачных сервисов разработана в соответствии с требованиями Федерального государственного стандарта среднего профессионального образования по специальности среднего профессионального образования программы подготовки специалистов среднего 09.02.06 Сетевое и системное администрирование, утвержденного приказом Минобрнауки РФ от 10.07.2023 №519.

Разработчики: Р.С. Реуцкий, преподаватель КСД ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № ____ от « ____ » _____ 20 ____ г.

Председатель ЦМК _____ Е.А. Стефанович
подпись

1 Общие сведения

Контрольно-оценочные средства (далее – КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины МДК.03.02 Безопасность облачных сервисов.

КОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта.

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ПК 3.5	У1	разрабатывать и внедрять процессы проверки подлинности на уровне подразделения и компании в целом, контролировать доступ к системе управления общедоступным облаком
ПК 3.5	У2	использовать общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости
ПК 3.5	У3	проводить постоянные проверки отказоустойчивости и восстановления системы
ПК 3.6	У4	внедрение решений для мониторинга с целью формирования предупреждений и автоматизации реагирования на различные инциденты
ПК 3.6	У5	поддерживать облачные конфигурации в актуальном состоянии и вести учет контроля версий
ПК 3.6	У6	внедрять централизованный сбор и анализ метрик для системной, сетевой и прикладной информации
ПК 3.6	У7	проводить постоянные проверки отказоустойчивости и восстановления системы
ПК 3.5	31	методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам
ПК 3.5	32	важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений
ПК 3.5	33	требования к совместимости компонентов внутри облачной инфраструктуры
ПК 3.5	34	методики и возможности автоматизации, широко используемые в техническом сообществе
ПК 3.5	35	сетевой поток данных и соответствующая зависимость доступности систем
ПК 3.5	36	требования к производительности и возможные узкие места при проектировании инфраструктуры
ПК 3.6	37	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами
ПК 3.6	38	важность и назначение сетевого трафика, а также изоляцию ресурсов
ПК 3.6	39	различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками
ПК 3.6	310	сетевой поток данных и соответствующая зависимость доступности систем
ПК 3.6	311	как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ПК 3.6	312	требования к производительности и возможные узкие места при проектировании инфраструктуры

3 Соответствие оценочных средств контролируемым результатам обучения

3.1 Средства, применяемые для оценки уровня теоретической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
Раздел 1. Технологии виртуализации и автоматизации.				
Тема 2.1. Основы и архитектура безопасности облачных сервисов	У1, У2, 31, 32, 33, 34, 35, 36	Определяет понятие и особенности безопасности облачных сервисов, объясняет задачи и цели защиты данных в облаке, характеризует модели ответственности (Shared Responsibility Model), разграничивает роли провайдера и клиента, анализирует основные угрозы и уязвимости облачных сервисов, интерпретирует требования стандартов и нормативных документов, разрабатывает и внедряет процессы проверки подлинности на уровне подразделения и компании в целом, контролирует доступ к системе управления общедоступным облаком, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, объясняет методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений, учитывает требования к совместимости компонентов внутри облачной инфраструктуры, применяет методики и возможности автоматизации, широко используемые в техническом сообществе, анализирует сетевой поток данных и соответствующую зависимость доступности систем, учитывает требования к производительности и	Устный опрос (п. 5.1, вопросы 1–10); Реферат (п. 5.2, темы 1–10); Тест №1 (п. 5.3); Тест №2 (п. 5.3)	Экзаменационные билеты №1–6 (п. 6.1)

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
		возможные узкие места при проектировании инфраструктуры.		
Тема 2.2. Технологии защиты и устойчивость инфраструктуры	У2, У3, У4, У5, У6, У7, 35, 36, 37, 38, 39, 310, 311, 312	Характеризует безопасность виртуальных машин и контейнеров, объясняет сетевые политики и сегментацию, сравнивает технологии VPN и защищённых соединений, анализирует способы защиты от DoS и DDoS атак, объясняет назначение IDS/IPS, систем мониторинга и централизованного сбора логов, интерпретирует подходы к резервному копированию, восстановлению данных и обеспечению высокой доступности, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, проводит постоянные проверки отказоустойчивости и восстановления системы, внедряет решения для мониторинга с целью формирования предупреждений и автоматизации реагирования на различные инциденты, поддерживает облачные конфигурации в актуальном состоянии и ведет учет контроля версий, внедряет централизованный сбор и анализ метрик для системной, сетевой и прикладной информации, объясняет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, раскрывает важность и назначение сетевого трафика, а также изоляцию ресурсов, анализирует различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые	Устный опрос (п. 5.1, вопросы 11–21); Реферат (п. 5.2, темы 11–20); Тест №3 (п. 5.3); Тест №4 (п. 5.3)	Экзаменационные билеты №7–17 (п. 6.1)

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
		поставщиками, учитывает сетевой поток данных и соответствующую зависимость доступности систем, объясняет, как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры.		
Тема 2.3. Управление доступом и эксплуатация защищённых решений	У1, У2, У4, У5, У6, У7, 31, 34, 37, 38, 39, 310, 311, 312	Объясняет политики доступа и IAM, характеризует безопасную эксплуатацию IaaS, PaaS, SaaS, раскрывает назначение тестовых и изолированных сред, объясняет принципы DevSecOps и безопасности CI/CD, сравнивает методы тестирования безопасности, интерпретирует процессы реагирования на инциденты и документирования политики безопасности, разрабатывает и внедряет процессы проверки подлинности на уровне подразделения и компании в целом, контролирует доступ к системе управления общедоступным облаком, использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, внедряет решения для мониторинга с целью формирования предупреждений и автоматизации реагирования на различные инциденты, поддерживает облачные конфигурации в актуальном состоянии и ведет учет контроля версий, внедряет централизованный сбор и анализ метрик для системной, сетевой и прикладной информации, проводит постоянные проверки отказоустойчивости и восстановления системы,	Устный опрос (п. 5.1, вопросы 22–30); Реферат (п. 5.2, темы 21–30); Тест №5 (п. 5.3)	Экзаменационные билеты №18–30 (п. 6.1)

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
		объясняет методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам, применяет методики и возможности автоматизации, широко используемые в техническом сообществе, объясняет различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами, раскрывает важность и назначение сетевого трафика, а также изоляцию ресурсов, анализирует различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками, объясняет, как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры.		

² - для формулировки показателей использовать положения Таксономии Блума.

³ - Однотипные оценочные средства нумеруются, н-р: «Тест №2», «Контрольная работа №4».

⁴ - Примеры всех оценочных средств должны быть представлены в разделах 5,6.

⁵ - В скобках следует указать пункт разделов 5.6, в котором оно представлено.

3.2 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Раздел 1. Технологии виртуализации и автоматизации.				

Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 1 Модели облачных сервисов: Анализ IaaS, PaaS, SaaS. Определение зон ответственности	У1, 31, 32	Разрабатывает и внедряет процессы проверки подлинности на уровне подразделения и компании в целом, контролирует доступ к системе управления общедоступным облаком, применяет методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам, раскрывает важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений, выполняет анализ IaaS, PaaS, SaaS, определение зон ответственности.	Тест №1 (п. 5.3)	Практическое задание экзаменационного билета №1 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 2 Анализ угроз облачных сервисов: Работа с базами уязвимостей (CVE, NVD)	У2, 33, 36	Использует общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости, учитывает требования к совместимости компонентов внутри облачной инфраструктуры, учитывает требования к производительности и возможные узкие места при проектировании инфраструктуры, выполняет анализ угроз облачных сервисов: работа с базами уязвимостей (CVE, NVD).	Тест №1 (п. 5.3)	Практическое задание экзаменационного билета №2 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 3 Настройка MFA: Подключение многофакторной аутентификации для пользователей	У1, 34	Разрабатывает и внедряет процессы проверки подлинности на уровне подразделения и компании в целом, контролирует доступ к системе управления общедоступным облаком, применяет методики и возможности автоматизации, широко используемые в техническом сообществе, выполняет настройку MFA для пользователей	Устный опрос (п. 5.1, вопросы 10–12); Реферат (п. 5.2, темы 10–11); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №5 (п. 6.1)

Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 4 Создание пользователей и ролей: Настройка RBAC, проверка разграничения прав	У1, 32, 34	Разрабатывает и внедряет процессы проверки подлинности, контролирует доступ, применяет требования к совместимости компонентов внутри облачной инфраструктуры, использует методики автоматизации, выполняет настройку RBAC и проверку разграничения прав	Устный опрос (п. 5.1, вопросы 11–12); Реферат (п. 5.2, темы 10–11); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №5 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 5 Шифрование данных: Настройка SSL/TLS, работа с сертификатами	У2, 35, 36	Использует облачные службы с учетом требований безопасности, анализирует сетевой поток данных, учитывает требования к производительности, выполняет настройку SSL/TLS и работу с сертификатами	Устный опрос (п. 5.1, вопросы 13–14); Реферат (п. 5.2, темы 12–13); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №6 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 6 Создание защищённого канала: Настройка PKI и VPN соединений	У2, 35	Использует облачные службы и защищённые соединения, анализирует сетевые зависимости, выполняет настройку PKI и VPN	Устный опрос (п. 5.1, вопросы 15); Реферат (п. 5.2, темы 14); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №7 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 7 Подготовка схемы облачной архитектуры: Обозначение точек уязвимости, построение схемы	У1, У2, 31, 32, 36	Проектирует архитектуру безопасности, определяет уязвимости, учитывает требования к инфраструктуре и совместимости, выполняет построение схемы облачной архитектуры	Устный опрос (п. 5.1, вопросы 9–10); Реферат (п. 5.2, темы 8–9); Тест №1 (п. 5.3)	Практическое задание экзаменационного билета №4 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов	У3, 36	Проводит проверки отказоустойчивости и восстановления системы, учитывает требования к	Устный опрос (п. 5.1, вопросы 25); Реферат (п.	Практическое задание

Практическое занятие № 8 Резервное копирование данных: Настройка snapshot и restore виртуальных машин		инфраструктуре, выполняет настройку snapshot и restore	5.2, темы 25); Тест №4 (п. 5.3)	экзаменационного билета №17 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 9 Контроль целостности данных: Проверка checksum, хэш- функции	У2, 35	Использует методы контроля целостности данных, анализирует сетевые зависимости, выполняет проверку checksum и хэш-функций	Устный опрос (п. 5.1, вопросы 16); Реферат (п. 5.2, темы 15); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №8 (п. 6.1)
Тема 2.1. Основы и архитектура безопасности облачных сервисов Практическое занятие № 10 Аудит базовых настроек безопасности: Составление отчета по проверке облачного сервиса	У1, 31, 36	Проводит аудит безопасности, анализирует требования и уязвимости, документирует результаты, составляет отчет по проверке	Устный опрос (п. 5.1, вопросы 9); Реферат (п. 5.2, темы 8); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №9 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивость инфраструктуры Практическое занятие № 1 Настройка сегментации сети: Создание VLAN и межсетевых сегментов	У6, 37, 38	Внедряет централизованный сбор и анализ метрик, использует различные сетевые архитектуры и изоляция ресурсов, выполняет настройку сегментации сети	Устный опрос (п. 5.1, вопросы 18–19); Реферат (п. 5.2, темы 17–18); Тест №3 (п. 5.3)	Практическое задание экзаменационного билета №11 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивость инфраструктуры Практическое занятие № 2 Правила firewall для облачной сети: Правила firewall для облачной сети	У4, 38	Внедряет решения для мониторинга и защиты, применяет механизмы фильтрации трафика, выполняет настройку firewall	Устный опрос (п. 5.1, вопросы 19); Реферат (п. 5.2, темы 18); Тест №3 (п. 5.3)	Практическое задание экзаменационного билета №11 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивость инфраструктуры Практическое занятие № 3 Настройка NAT и VPN: Подключение защищённых туннелей между сегментами	У4, 310	Внедряет защищённые соединения, анализирует сетевой поток данных, выполняет настройку NAT и VPN	Устный опрос (п. 5.1, вопросы 20); Реферат (п. 5.2, темы 19); Тест №3 (п. 5.3)	Практическое задание экзаменационного билета №12 (п. 6.1)
Тема 2.2. Технологии защиты и	У4, У6, 311	Внедряет системы мониторинга и анализа метрик,	Устный опрос (п. 5.1,	Практическое

устойчивость инфраструктуры Практическое занятие № 4 Конфигурация IDS/IPS: Настройка Suricata или Snort для обнаружения атак		использует IDS/IPS, выполняет настройку Suricata или Snort	вопросы 22); Реферат (п. 5.2, темы 21–22); Тест №4 (п. 5.3)	задание экзаменационного билета №14 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивости инфраструктуры Практическое занятие № 5 Централизованный сбор логов: Настройка ELK или Grafana Loki	У6, 311	Внедряет централизованный сбор логов, анализирует метрики, выполняет настройку ELK или Grafana Loki	Устный опрос (п. 5.1, вопросы 23–24); Реферат (п. 5.2, темы 23–24); Тест №4 (п. 5.3)	Практическое задание экзаменационного билета №15 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивости инфраструктуры Практическое занятие № 6 Анализ журналов безопасности: Выявление подозрительных событий	У4, 311	Анализирует журналы безопасности, выявляет инциденты, применяет метрики для оценки состояния системы	Устный опрос (п. 5.1, вопросы 23–24); Реферат (п. 5.2, темы 23–24); Тест №4 (п. 5.3)	Практическое задание экзаменационного билета №16 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивости инфраструктуры Практическое занятие № 7 Настройка защиты от DoS/DDoS: Rate limiting, Fail2Ban, Cloudflare	У4, 39	Внедряет механизмы защиты от атак, использует средства ограничения трафика, выполняет настройку защиты от DoS/DDoS	Устный опрос (п. 5.1, вопросы 21); Реферат (п. 5.2, темы 20); Тест №3 (п. 5.3)	Практическое задание экзаменационного билета №13 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивости инфраструктуры Практическое занятие № 8 Настройка резервного копирования: Репликация данных, инкрементальные бэкапы	У7, 312	Проводит проверки отказоустойчивости, учитывает требования к производительности, выполняет настройку резервного копирования	Устный опрос (п. 5.1, вопросы 25); Реферат (п. 5.2, темы 25); Тест №4 (п. 5.3)	Практическое задание экзаменационного билета №17 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивости инфраструктуры Практическое занятие № 9 Настройка высокой доступности: HAProxy, Keepalived, балансировка нагрузки	У7, 39	Обеспечивает отказоустойчивость, использует балансировку нагрузки, выполняет настройку HAProxy и Keepalived	Устный опрос (п. 5.1, вопросы 26); Реферат (п. 5.2, темы 26); Тест №4 (п. 5.3)	Практическое задание экзаменационного билета №18 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивости инфраструктуры	У7, 312	Проводит тестирование восстановления системы, анализирует отказоустойчивость, выполняет	Устный опрос (п. 5.1, вопросы 25); Реферат (п.	Практическое задание

Практическое занятие № 10 Тестирование Disaster Recovery: Проверка восстановления сервисов		проверку DR	5.2, темы 25); Тест №4 (п. 5.3)	экзаменационного билета №17 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивость инфраструктуры Практическое занятие № 11 Мониторинг состояния инфраструктуры: Настройка Prometheus/Grafana	У6, 311	Внедряет мониторинг, анализирует метрики, выполняет настройку Prometheus/Grafana	Устный опрос (п. 5.1, вопросы 22–23); Реферат (п. 5.2, темы 21–23); Тест №4 (п. 5.3)	Практическое задание экзаменационного билета №15 (п. 6.1)
Тема 2.2. Технологии защиты и устойчивость инфраструктуры Практическое занятие № 12 Настройка политики хранения логов: Автоматическая ротация и архивирование	У5, 311	Поддерживает конфигурации, управляет логами, выполняет настройку политики хранения и ротации	Устный опрос (п. 5.1, вопросы 23); Реферат (п. 5.2, темы 23); Тест №4 (п. 5.3)	Практическое задание экзаменационного билета №15 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 1 Создание политики IAM: Настройка пользователей и ролей	У1, 31	Разрабатывает политики доступа, взаимодействует с бизнес-единицами, выполняет настройку IAM	Устный опрос (п. 5.1, вопросы 27); Реферат (п. 5.2, темы 27); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №19 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 2 Разграничение прав в Kubernetes / Proxmox: Практика RBAC	У1, 33	Реализует разграничение прав, учитывает совместимость компонентов, выполняет настройку RBAC	Устный опрос (п. 5.1, вопросы 11); Реферат (п. 5.2, темы 10); Тест №2 (п. 5.3)	Практическое задание экзаменационного билета №5 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 3 Развёртывание тестовой среды (sandbox): Изолированная среда для проверки ПО	У2, 32	Использует облачные сервисы, учитывает инфраструктуру, выполняет развёртывание sandbox среды	Устный опрос (п. 5.1, вопросы 21); Реферат (п. 5.2, темы 21); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №21 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие	У5, 34	Поддерживает конфигурации, применяет автоматизацию, внедряет DevSecOps	Устный опрос (п. 5.1, вопросы 28); Реферат (п. 5.2, темы 28); Тест №5	Практическое задание экзаменационного

№ 4 Безопасный конвейер CI/CD: Настройка сканирования уязвимостей			(п. 5.3)	билета №22 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 5 Сканирование контейнеров: Trivy, Clair, проверка образов	У4, 36	Выполняет анализ уязвимостей, учитывает производительность, применяет инструменты сканирования	Устный опрос (п. 5.1, вопросы 29); Реферат (п. 5.2, темы 29); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №24 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 6 Vulnerability Scanning: Анализ и устранение уязвимостей	У4, 36	Проводит анализ уязвимостей, выявляет угрозы, применяет методы сканирования	Устный опрос (п. 5.1, вопросы 29); Реферат (п. 5.2, темы 29); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №23 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 7 Проведение pentest облачного сервиса: Использование OWASP Top 10	У4, 36	Проводит тестирование безопасности, анализирует угрозы, выполняет pentest	Устный опрос (п. 5.1, вопросы 29); Реферат (п. 5.2, темы 29); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №23 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 8 Реагирование на инциденты: Практика Incident Response Workflow	У4, 31	Реализует процессы реагирования, взаимодействует с заинтересованными сторонами	Устный опрос (п. 5.1, вопросы 30); Реферат (п. 5.2, темы 30); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №25 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 9 Настройка уведомлений и алертов: Автоматические оповещения о событиях	У4, 311	Внедряет автоматическое реагирование, использует метрики, выполняет настройку алертов	Устный опрос (п. 5.1, вопросы 30); Реферат (п. 5.2, темы 30); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №26 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 10 Документирование	У1, 31	Разрабатывает документы безопасности, взаимодействует с бизнесом, оформляет регламенты	Устный опрос (п. 5.1, вопросы 30); Реферат (п. 5.2, темы 30); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №27 (п. 6.1)

политики безопасности: Создание шаблонов и регламентов				
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 11 Проверка соответствия стандартам: Сравнение с ISO/IEC 27017, GDPR	У2, 31	Анализирует соответствие стандартам, взаимодействует с бизнесом, оценивает требования	Устный опрос (п. 5.1, вопросы 7–8); Реферат (п. 5.2, темы 6–7); Тест №1 (п. 5.3)	Практическое задание экзаменационного билета №28 (п. 6.1)
Тема 2.3. Управление доступом и эксплуатация защищённых решений Практическое занятие № 12 Настройка аудита действий пользователей: Логирование и контроль доступа	У1, 31	Реализует аудит действий, контролирует доступ, анализирует события	Устный опрос (п. 5.1, вопросы 29); Реферат (п. 5.2, темы 29); Тест №5 (п. 5.3)	Практическое задание экзаменационного билета №29 (п. 6.1)

4 Описание процедуры оценивания

Результаты обучения по дисциплине, уровень сформированности компетенций оцениваются по четырём бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом.

Критерии оценивания устного ответа

Оценочные средства: собеседование, устное сообщение

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

Оценочные средства: доклад (сообщение), в том числе выполненный в форме презентации.

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера.

Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	<i>Отлично</i>	<i>Хорошо</i>	<i>Удовлетворительно</i>	<i>Неудовлетворительно</i>
Количество правильных ответов	91 % и $\geq$	от 81% до 90,9 %	не менее 70%	менее 70%

Критерии выставления оценки студенту на зачете/ экзамене

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только

	основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

1. Что понимается под безопасностью облачных сервисов?
2. Каковы основные задачи и цели защиты данных в облаке?
3. В чем заключается модель ответственности Shared Responsibility Model?
4. Как распределяются роли провайдера и клиента в модели ответственности облачных сервисов?
5. Какие основные угрозы и уязвимости характерны для облачных сервисов?
6. Для чего используются базы уязвимостей CVE и NVD?
7. Какие стандарты и нормативные требования применяются к безопасности облачных сервисов?
8. Какую роль играют ISO/IEC 27017, ISO/IEC 27018, GDPR и ФЗ-152 в защите облачных данных?
9. Что включает в себя архитектура облачной безопасности?
10. Какие меры применяются для защиты данных, сетей, пользователей и приложений в облаке?
11. Для чего используются MFA, RBAC, OAuth2, OpenID Connect и SAML?
12. В чем заключается значение многофакторной аутентификации для безопасности облачных сервисов?
13. Какие технологии применяются для шифрования данных при хранении и передаче?
14. В чем различие между SSL/TLS, AES и PGP?
15. Для чего применяются PKI и VPN при защите облачной инфраструктуры?
16. Как выполняется контроль целостности данных с использованием checksum и хэш-функций?
17. Какие меры безопасности используются для защиты виртуальных машин и контейнеров?
18. Что такое сетевые политики и сегментация в облачной инфраструктуре?
19. Для чего применяются VLAN, Security Groups, Firewall и NAT?
20. Какие технологии используются для организации VPN и защищённых соединений?
21. Какие способы защиты применяются от DoS и DDoS атак?
22. Для чего используются Suricata, Snort, WAF и системы логирования?
23. В чем состоит значение централизованного сбора логов в облачной инфраструктуре?
24. Для чего используются ELK и Grafana Loki при анализе событий безопасности?
25. Какие подходы применяются для резервного копирования и восстановления данных в облаке?

26. В чем состоит роль HAProxy, Keepalived и балансировки нагрузки при обеспечении высокой доступности?
27. Что включает в себя политика доступа и IAM в облачных сервисах?
28. Что такое DevSecOps и как безопасность интегрируется в CI/CD?
29. Какие методы тестирования безопасности используются в облачной инфраструктуре?
30. Что включает в себя реагирование на инциденты и документирование политики безопасности в облачных сервисах?

5.2 Темы рефератов

1. Безопасность облачных сервисов: понятие, особенности, задачи и цели защиты данных в облаке
2. Модели ответственности в облачных сервисах: Shared Responsibility Model
3. Распределение ролей провайдера и клиента в обеспечении безопасности облачных сервисов
4. Основные угрозы и уязвимости облачных сервисов
5. Использование баз уязвимостей CVE и NVD в анализе безопасности облачных сервисов
6. Стандарты и нормативные требования в области безопасности облачных сервисов
7. Применение ISO/IEC 27017, ISO/IEC 27018, GDPR и ФЗ-152 для защиты облачных данных
8. Архитектура безопасности облачных сервисов
9. Защита данных, сетей, пользователей и приложений в облачной инфраструктуре
10. Многофакторная аутентификация и управление доступом в облачных сервисах
11. Технологии MFA, RBAC, OAuth2, OpenID Connect и SAML в облачной безопасности
12. Технологии шифрования данных при хранении и передаче в облачной среде
13. Применение SSL/TLS, AES и PGP для защиты информации в облачных сервисах
14. PKI и VPN как средства построения защищённых каналов связи
15. Контроль целостности данных в облачных сервисах: checksum и хэш-функции
16. Безопасность виртуальных машин и контейнеров в облачной инфраструктуре
17. Сетевые политики и сегментация в облачной среде
18. VLAN, Security Groups, Firewall и NAT как инструменты защиты облачной сети
19. VPN и защищённые соединения в облачной инфраструктуре: IPsec, WireGuard, SSL-VPN
20. Защита облачных сервисов от DoS и DDoS атак
21. Системы мониторинга и IDS/IPS в защите облачной инфраструктуры
22. Suricata, Snort и WAF как инструменты обнаружения и предотвращения атак
23. Централизованный сбор логов и аудит событий безопасности в облачной инфраструктуре
24. Использование ELK и Grafana Loki для анализа журналов безопасности
25. Резервное копирование, репликация и Disaster Recovery в облачных сервисах
26. Высокая доступность облачной инфраструктуры: HAProxy, Keepalived и балансировка нагрузки
27. Политики доступа и IAM в облачных сервисах
28. DevSecOps и безопасность CI/CD в облачной инфраструктуре
29. Методы тестирования безопасности облачных сервисов: Vulnerability Scanning, Pentest, OWASP Top 10
30. Реагирование на инциденты и документирование политики безопасности в облачных сервисах

5.3 Примеры тестовых заданий

Тест №1

1. Что наиболее точно характеризует безопасность облачных сервисов?
 - а) Защиту только сетевых подключений
 - б) Защиту данных, сервисов и доступа в облачной среде (верно)
 - в) Резервирование только физических серверов
 - г) Контроль только действий администратора

2. В модели Shared Responsibility Model клиент обычно отвечает за:
 - а) Настройку доступа к своим данным и сервисам (верно)
 - б) Охрану дата-центра провайдера
 - в) Замену сетевого оборудования провайдера
 - г) Электропитание облачной платформы

3. Что обычно относится к зоне ответственности провайдера?
 - а) Политики доступа внутри организации клиента
 - б) Защита физической инфраструктуры облака (верно)
 - в) Проверка внутренних регламентов клиента
 - г) Назначение ролей сотрудникам заказчика

4. Для чего используется база CVE?
 - а) Для поиска известных уязвимостей (верно)
 - б) Для генерации TLS-сертификатов
 - в) Для хранения резервных копий
 - г) Для настройки журналирования

5. Чем NVD полезна по сравнению с простым перечнем CVE?
 - а) Содержит расширенную информацию об уязвимостях (верно)
 - б) Используется только для шифрования
 - в) Хранит контейнерные образы
 - г) Применяется вместо firewall

6. Какой стандарт теснее связан с защитой персональных данных в облаке?
 - а) ISO/IEC 27018 (верно)
 - б) ISO/IEC 27017
 - в) CVE
 - г) NVD

7. Что включает архитектура облачной безопасности?
 - а) Только VPN и firewall
 - б) Только управление паролями
 - в) Защиту данных, сетей, пользователей и приложений (верно)
 - г) Только аудит уязвимостей

8. Для чего применяется MFA?
 - а) Для шифрования хранилища
 - б) Для подтверждения личности несколькими факторами (верно)
 - в) Для настройки сетевой сегментации
 - г) Для публикации контейнеров

9. Основная задача RBAC — это:
 - а) Разграничение прав по ролям (верно)
 - б) Шифрование канала связи

- в) Сжатие логов безопасности
- г) Балансировка нагрузки

10. Где уместнее всего применять OAuth2?

- а) При выдаче ограниченного доступа приложению (верно)
- б) При настройке виртуального коммутатора
- в) При создании snapshot виртуальной машины
- г) При настройке VLAN между узлами

Время выполнения – 10 минут

Тест №2

1. Что в первую очередь обеспечивает SSL/TLS?

- а) Защиту передачи данных по сети (верно)
- б) Проверку целостности диска
- в) Изоляцию контейнеров
- г) Управление ролями пользователей

2. Для чего чаще всего применяется AES?

- а) Для симметричного шифрования данных (верно)
- б) Для публикации образов контейнеров
- в) Для маршрутизации трафика
- г) Для настройки резервирования

3. Что характерно для PGP?

- а) Использование для защиты и подписи данных (верно)
- б) Работа только как VPN-протокол
- в) Использование только в Kubernetes
- г) Замена RBAC в облаке

4. Для чего применяется PKI?

- а) Для управления доверием на основе сертификатов (верно)
- б) Для балансировки сетевой нагрузки
- в) Для резервирования виртуальных машин
- г) Для хранения событий аудита

5. Что дает VPN между сегментами инфраструктуры?

- а) Защищённый канал связи (верно)
- б) Повышение частоты процессора
- в) Автоматическую проверку уязвимостей
- г) Развертывание контейнеров

6. Что означает контроль целостности данных?

- а) Проверку отсутствия изменений в данных (верно)
- б) Проверку числа подключений к серверу
- в) Настройку политик доступа
- г) Обновление сертификатов

7. Для чего используется checksum?

- а) Для проверки неизменности данных (верно)
- б) Для фильтрации трафика

- в) Для назначения ролей
- г) Для сжатия журналов

8. Что делает хэш-функция в задачах безопасности?

- а) Формирует контрольное значение данных (верно)
- б) Выдает IP-адрес узлу
- в) Настраивает VPN-туннель
- г) Управляет репликацией данных

9. В чем цель аудита базовых настроек безопасности?

- а) В выявлении небезопасных конфигураций (верно)
- б) В увеличении производительности сети
- в) В публикации контейнерных образов
- г) В резервировании CPU и RAM

10. Зачем составляется отчет по проверке облачного сервиса?

- а) Для фиксации результатов и замечаний (верно)
- б) Для переноса VM между узлами
- в) Для настройки DHCP
- г) Для создания снимка состояния

Время выполнения – 10 минут

Тест №3

1. Что является важной мерой защиты виртуальных машин и контейнеров?

- а) Изоляция и контроль доступа (верно)
- б) Только замена гипервизора
- в) Только резервирование питания
- г) Только увеличение объема памяти

2. Для чего применяется VLAN?

- а) Для логического разделения трафика (верно)
- б) Для шифрования файлов
- в) Для настройки образов Docker
- г) Для аудита пользователей

3. Какую задачу решают Security Groups?

- а) Контролируют сетевой доступ по правилам (верно)
- б) Управляют резервным копированием
- в) Формируют хэш-суммы файлов
- г) Выполняют репликацию контейнеров

4. Основное назначение firewall — это:

- а) Фильтрация сетевого трафика (верно)
- б) Управление сертификатами
- в) Публикация контейнеров
- г) Назначение ролей

5. Что делает NAT?

- а) Преобразует сетевые адреса (верно)
- б) Шифрует содержимое дисков

- в) Выполняет аудит пользователей
 - г) Управляет токенами доступа
6. Какой вариант относится к защищённым VPN-технологиям?
- а) WireGuard (верно)
 - б) SMTP
 - в) YAML
 - г) PNG
7. Для чего применяется rate limiting?
- а) Для ограничения потока запросов (верно)
 - б) Для создания сертификатов
 - в) Для хранения логов
 - г) Для назначения ролей
8. Какую задачу решает Fail2Ban?
- а) Автоматически блокирует подозрительные обращения (верно)
 - б) Выполняет балансировку нагрузки
 - в) Проводит шифрование базы данных
 - г) Управляет контейнерными томами
9. Что делает WAF?
- а) Защищает веб-приложение на уровне HTTP/HTTPS (верно)
 - б) Управляет снапшотами виртуальных машин
 - в) Настраивает RAID-массив
 - г) Публикует контейнеры в registry
10. Что относится к защите от DoS и DDoS атак?
- а) Rate limit, Fail2Ban, WAF, Cloudflare (верно)
 - б) Docker Compose, YAML, Registry, Image
 - в) RBAC, SAML, OAuth2, OpenID Connect
 - г) Snapshot, restore, checksum, hash

Время выполнения – 10 минут

Тест №4

1. Для чего применяются Suricata и Snort?
- а) Для обнаружения подозрительного сетевого трафика (верно)
 - б) Для настройки резервирования CPU
 - в) Для публикации образов Docker
 - г) Для балансировки HTTP-запросов
2. Что дает централизованный сбор логов?
- а) Сводный анализ событий из разных источников (верно)
 - б) Только ускорение запуска приложений
 - в) Только настройку сертификатов
 - г) Только фильтрацию DNS-запросов
3. Какой стек часто используют для сбора и анализа логов?
- а) ELK (верно)
 - б) LAMP

- в) KVM
- г) NAT

4. Для чего применяется Grafana Loki?

- а) Для работы с журналами событий (верно)
- б) Для настройки виртуального BIOS
- в) Для управления RBAC
- г) Для контроля snapshot виртуальных машин

5. Что позволяет анализ журналов безопасности?

- а) Выявлять подозрительные действия и события (верно)
- б) Только увеличивать скорость сети
- в) Только добавлять новых пользователей
- г) Только обновлять контейнеры

6. Что относится к резервному копированию в облаке?

- а) Snapshot и репликация (верно)
- б) VLAN и NAT
- в) RBAC и MFA
- г) WAF и IDS

7. Что означает Disaster Recovery?

- а) Восстановление после сбоев и аварий (верно)
- б) Метод ограничения трафика
- в) Подход к созданию контейнеров
- г) Способ назначения ролей

8. Для чего используется HAProxy?

- а) Для балансировки нагрузки (верно)
- б) Для выпуска сертификатов
- в) Для аудита контейнеров
- г) Для хэширования данных

9. Какую роль выполняет Keepalived?

- а) Помогает обеспечить отказоустойчивость сервисов (верно)
- б) Проводит проверку CVE
- в) Настраивает шифрование на диске
- г) Управляет образами Docker

10. Что дает высокая доступность инфраструктуры?

- а) Снижение риска простоя сервисов (верно)
- б) Удаление журналов безопасности
- в) Отказ от резервного копирования
- г) Отключение сетевой сегментации

Время выполнения – 10 минут

Тест №5

1. Что включает IAM в облачных сервисах?

- а) Управление пользователями, ролями и доступом (верно)
- б) Только настройку сетевых коммутаторов

- в) Только резервирование баз данных
 - г) Только мониторинг контейнеров
2. Для чего создают sandbox-среду?
- а) Для изолированного тестирования изменений (верно)
 - б) Для хранения резервных копий
 - в) Для публикации сертификатов
 - г) Для увеличения пропускной способности сети
3. Что означает DevSecOps?
- а) Встраивание безопасности в процессы разработки и доставки (верно)
 - б) Полный отказ от автоматизации
 - в) Только ручную проверку журналов
 - г) Только физическую защиту серверов
4. Для чего в CI/CD добавляют сканирование уязвимостей?
- а) Для поиска проблем безопасности до развертывания (верно)
 - б) Для ускорения генерации логов
 - в) Для настройки VPN-подключений
 - г) Для управления VLAN
5. Для чего применяются Trivy и Clair?
- а) Для анализа контейнерных образов на уязвимости (верно)
 - б) Для балансировки трафика
 - в) Для настройки PKI
 - г) Для шифрования журналов
6. Что является целью Vulnerability Scanning?
- а) Выявление известных уязвимостей в системе (верно)
 - б) Подмена IP-адресов в сети
 - в) Публикация приложений в облаке
 - г) Настройка высокой доступности
7. Что обычно включает pentest облачного сервиса?
- а) Проверку системы на возможные векторы атаки (верно)
 - б) Только резервное копирование логов
 - в) Только назначение ролей
 - г) Только настройку коммутаторов
8. Что означает Incident Response Workflow?
- а) Порядок реагирования на инциденты безопасности (верно)
 - б) Схему развертывания виртуальных машин
 - в) Алгоритм маршрутизации трафика
 - г) Порядок обновления гипервизора
9. Для чего настраивают уведомления и алерты?
- а) Для автоматического оповещения о событиях (верно)
 - б) Для увеличения объема хранилища
 - в) Для ручного управления VLAN
 - г) Для создания PKI без сертификатов

10. Для чего нужно документирование политики безопасности?

- а) Для фиксации требований, правил и регламентов (верно)
- б) Для удаления журналов после проверки
- в) Для отказа от RBAC
- г) Для отключения аудита действий пользователей

Время выполнения – 10 минут

6. Примеры оценочных средств для проведения промежуточной аттестации

6.1 Варианты экзаменационных билетов:

Экзаменационный билет №1

1. Понятие и особенности безопасности облачных сервисов. Основные задачи и цели защиты данных в облаке.
2. Модели ответственности (Shared Responsibility Model). Роли провайдера и клиента, примеры.

Практическое задание:

Проанализировать выбранный облачный сервис и определить, какие функции безопасности относятся к зоне ответственности провайдера, а какие — к зоне ответственности клиента. Представить результат в виде краткой схемы или таблицы.

Экзаменационный билет №2

1. Основные угрозы и уязвимости облачных сервисов. Классификация угроз.
2. Использование баз уязвимостей CVE и NVD при анализе безопасности облачной инфраструктуры.

Практическое задание:

Найти в открытых источниках пример уязвимости облачного компонента, определить её идентификатор CVE, кратко описать угрозу и предложить меры по снижению риска.

Экзаменационный билет №3

1. Стандарты и нормативные требования в безопасности облачных сервисов.
2. ISO/IEC 27017, ISO/IEC 27018, GDPR, ФЗ-152: назначение и области применения.

Практическое задание:

Сравнить два нормативных документа из списка ISO/IEC 27017, ISO/IEC 27018, GDPR, ФЗ-152 и указать, какие требования они предъявляют к защите облачных данных.

Экзаменационный билет №4

1. Архитектура облачной безопасности: защита данных, сетей, пользователей, приложений.
2. Взаимосвязь механизмов аутентификации, авторизации и сетевой защиты в облачной среде.

Практическое задание:

Подготовить схему облачной архитектуры с указанием точек уязвимости и предложить меры защиты для каждого элемента схемы.

Экзаменационный билет №5

1. MFA, RBAC, OAuth2, OpenID Connect, SAML: назначение и особенности применения.
2. Разграничение прав доступа пользователей в облачных сервисах.

Практическое задание:

Настроить модель разграничения доступа по ролям для трёх категорий пользователей и обосновать права, выданные каждой группе.

Экзаменационный билет №6

1. Технологии шифрования данных при хранении и передаче.
2. SSL/TLS, AES, PGP: различия, назначение, ограничения.

Практическое задание:

Предложить схему защиты данных облачного сервиса, в которой отдельно указаны механизмы защиты данных при передаче и при хранении.

Экзаменационный билет №7

1. PKI как основа доверенной инфраструктуры безопасности.
2. VPN-соединения в облачной среде: назначение, виды, преимущества и ограничения.

Практическое задание:

Разработать план настройки защищённого канала между двумя сегментами инфраструктуры с использованием PKI и VPN.

Экзаменационный билет №8

1. Контроль целостности данных в облачных сервисах.
2. Checksum, хэш-функции и их значение в обеспечении безопасности.

Практическое задание:

Продemonстрировать способ проверки целостности файла или резервной копии и описать, как обнаружить факт несанкционированного изменения данных.

Экзаменационный билет №9

1. Аудит базовых настроек безопасности облачного сервиса.
2. Основные этапы проверки конфигурации и документирования результатов аудита.

Практическое задание:

Составить структуру отчёта по проверке безопасности облачного сервиса, включив в него разделы по пользователям, доступу, шифрованию, резервному копированию и журналированию.

Экзаменационный билет №10

1. Безопасность виртуальных машин и контейнеров в облачной инфраструктуре.
2. Изоляция, настройка доступа и риски совместного использования ресурсов.

Практическое задание:

Сравнить меры защиты виртуальной машины и контейнера, выделить общие и специфические механизмы безопасности.

Экзаменационный билет №11

1. Сетевые политики и сегментация в облачной инфраструктуре.
2. VLAN, Security Groups, Firewall, NAT: назначение и совместное применение.

Практическое задание:

Разработать схему сегментации облачной сети для трёх сервисов с разными требованиями к доступу и взаимодействию.

Экзаменационный билет №12

1. VPN и защищённые соединения в облачной инфраструктуре.
2. IPsec, WireGuard, SSL-VPN: сравнение технологий и сценариев применения.

Практическое задание:

Выбрать подходящую технологию VPN для организации защищённого доступа сотрудников к облачному сервису и обосновать выбор.

Экзаменационный билет №13

1. Защита от DoS и DDoS атак в облачной среде.
2. Rate limit, Fail2Ban, Cloudflare, WAF: функции и границы применения.

Практическое задание:

Предложить комплекс мер по защите веб-приложения в облаке от DoS/DDoS атак с распределением функций между разными средствами защиты.

Экзаменационный билет №14

1. IDS/IPS в обеспечении безопасности облачной инфраструктуры.
2. Suricata, Snort, WAF, логирование: задачи и особенности применения.

Практическое задание:

Составить план внедрения IDS/IPS в облачную сеть с указанием места установки, типов контролируемого трафика и порядка реагирования на события.

Экзаменационный билет №15

1. Централизованный сбор логов в облачной инфраструктуре.
2. ELK, Grafana Loki, аудит событий: назначение и практическая ценность.

Практическое задание:

Разработать схему централизованного сбора логов для облачного сервиса и указать, какие источники логов должны быть подключены в первую очередь.

Экзаменационный билет №16

1. Анализ журналов безопасности и выявление подозрительных событий.
2. Признаки компрометации в логах пользователей, приложений и сетевой инфраструктуры.

Практическое задание:

По описанию событий определить, какие из них могут свидетельствовать о попытке атаки, и предложить первоочередные действия администратора.

Экзаменационный билет №17

1. Резервное копирование и восстановление данных в облачной инфраструктуре.
2. Snapshot, репликация, Disaster Recovery: различия и взаимосвязь.

Практическое задание:

Разработать схему резервного копирования сервиса с указанием периодичности, типа копий и порядка восстановления после сбоя.

Экзаменационный билет №18

1. Обеспечение высокой доступности облачной инфраструктуры.
2. HAProxy, Keepalived, балансировка нагрузки: принципы работы и практическое значение.

Практическое задание:

Предложить архитектуру отказоустойчивого веб-сервиса с балансировкой нагрузки и резервированием точки входа.

Экзаменационный билет №19

1. Политики доступа и IAM в облачных сервисах.
2. Создание пользователей, разграничение прав, RBAC.

Практическое задание:

Составить модель IAM для облачной инфраструктуры организации, в которой есть администраторы, разработчики, аудиторы и обычные пользователи.

Экзаменационный билет №20

1. Развёртывание инфраструктуры IaaS, PaaS, SaaS и особенности безопасной эксплуатации.
2. Риски безопасности в различных моделях облачных сервисов.

Практическое задание:

Для одного и того же бизнес-приложения определить, как будут меняться требования к безопасности при размещении в моделях IaaS, PaaS и SaaS.

Экзаменационный билет №21

1. Тестовые и изолированные среды в облачной инфраструктуре.
2. Sandbox для тестирования новых версий программного обеспечения и его роль в безопасности.

Практическое задание:

Разработать схему изолированной тестовой среды для проверки новой версии приложения с указанием ограничений доступа и сетевого взаимодействия.

Экзаменационный билет №22

1. DevSecOps и безопасность CI/CD.
2. Интеграция сканирования уязвимостей и автоматизации в жизненный цикл разработки.

Практическое задание:

Предложить набор проверок безопасности, которые должны быть встроены в конвейер CI/CD для контейнеризированного приложения.

Экзаменационный билет №23

1. Методы тестирования безопасности облачной инфраструктуры.
2. Vulnerability Scanning, Pentest, OWASP Top 10: назначение, различия, ограничения.

Практическое задание:

Составить план тестирования безопасности облачного веб-приложения, указав, какие методы и на каком этапе должны применяться.

Экзаменационный билет №24

1. Сканирование контейнеров и образов на уязвимости.
2. Trivy, Clair, проверка образов и интерпретация результатов сканирования.

Практическое задание:

Описать порядок анализа контейнерного образа на уязвимости и предложить действия по устранению найденных проблем.

Экзаменационный билет №25

1. Реагирование на инциденты в облачной инфраструктуре.
2. Incident Response Workflow: этапы, участники, порядок действий.

Практическое задание:

Разработать последовательность реагирования на инцидент, связанный с несанкционированным доступом к облачному сервису.

Экзаменационный билет №26

1. Настройка уведомлений и алертов в защищённой инфраструктуре.
2. Автоматические оповещения о событиях и их роль в своевременном реагировании.

Практическое задание:

Предложить набор критических событий безопасности, для которых должны быть настроены автоматические уведомления, и указать каналы их доставки.

Экзаменационный билет №27

1. Документирование политики безопасности облачного сервиса.
2. Создание шаблонов и регламентов в системе защиты информации.

Практическое задание:

Составить структуру документа «Политика безопасности облачного сервиса», включив в неё разделы по доступу, журналированию, резервному копированию и реагированию на инциденты.

Экзаменационный билет №28

1. Проверка соответствия стандартам в области облачной безопасности.
2. Сравнение практики эксплуатации облачного сервиса с требованиями ISO/IEC 27017 и GDPR.

Практическое задание:

Подготовить перечень контрольных вопросов для оценки соответствия облачного сервиса выбранному стандарту или нормативному документу.

Экзаменационный билет №29

1. Аудит действий пользователей и контроль доступа в облачной инфраструктуре.
2. Значение логирования пользовательской активности для безопасности и расследования инцидентов.

Практическое задание:

Разработать схему аудита действий пользователей для облачного сервиса, указав, какие события должны фиксироваться обязательно.

Экзаменационный билет №30

1. Проектирование защищённой облачной инфраструктуры.
2. Комплексное объединение механизмов защиты данных, сетей, пользователей, приложений и процессов реагирования.

Практическое задание:

Разработать концептуальную схему защищённой облачной инфраструктуры организации, включив в неё IAM, MFA, сегментацию сети, шифрование, централизованный сбор логов, резервное копирование, высокую доступность и порядок реагирования на инциденты.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА
для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

МДК.03.03 Технологии хранения и анализа данных

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2025

Контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине МДК.03.03 Технологии хранения и анализа данных разработана в соответствии с требованиями Федерального государственного стандарта среднего профессионального образования по специальности среднего профессионального образования программы подготовки специалистов среднего 09.02.06 Сетевое и системное администрирование, утвержденного приказом Минобрнауки РФ от 10.07.2023 №519.

Разработчики: Р.С. Реуцкий, преподаватель КСД ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № ____ от « ____ » _____ 20 ____ г.

Председатель ЦМК _____ Е.А. Стефанович
подпись

1 Общие сведения

Контрольно-оценочные средства (далее – КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины МДК.03.03 Технологии хранения и анализа данных.

КОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта.

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ПК 3.4	У1	документацию по организации сегментов сети
ПК 3.4	У2	контролировать соответствие разрабатываемого проекта нормативно-технической документации
ПК 3.4	У3	использовать программно-аппаратные средства технического контроля
ПК 3.4	У4	использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования
ПК 3.4	З1	требования к компьютерным сетям
ПК 3.4	З2	архитектуру протоколов
ПК 3.4	З3	стандартизацию сетей
ПК 3.4	З4	этапы проектирования сетевой инфраструктуры
ПК 3.4	З5	организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей
ПК 3.4	З6	стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы (монтаж, тестирование)
ПК 3.4	З7	средства тестирования и анализа
ПК 3.4	З8	программно-аппаратные средства технического контроля

3 Соответствие оценочных средств контролируемым результатам обучения

3.1 Средства, применяемые для оценки уровня теоретической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
Раздел 1. Технологии виртуализации и автоматизации.				
Тема 3.1 Инфраструктура и технологии хранения данных	У1, У2, У3, У4, 31, 32, 33, 34, 35, 36, 37, 38	Обучающийся объясняет назначение и особенности технологий хранения данных; различает архитектуры DAS, NAS, SAN, Unified Storage, SDS, HCI; анализирует принципы работы NFS, SMB, iSCSI, S3, RAID, InfiniBand; обосновывает выбор решений хранения с учётом требований производительности, отказоустойчивости, масштабируемости и безопасности; использует техническую документацию, стандарты, средства анализа и контроля для оценки и подбора инфраструктурных решений.	Устный опрос (п. 5.1, вопросы 1–20); Реферат (п. 5.2, темы 1–14); Тест №1 (п. 5.3); Тест №2 (п. 5.3)	Экзаменационные билеты №1–8 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных	У1, У2, У3, У4, 31, 32, 33, 34, 35, 37, 38	Обучающийся характеризует методы контроля целостности, резервного копирования, репликации, миграции и аудита данных; сравнивает MD5 и SHA, snapshot и backup, синхронную и асинхронную репликацию, rsync и rclone; анализирует механизмы ACL, POSIX и IAM; оценивает риски потери данных и способы обеспечения отказоустойчивости; применяет средства технического контроля и справочные материалы для выбора решений по защите и восстановлению данных.	Устный опрос (п. 5.1, вопросы 21–30); Реферат (п. 5.2, темы 15–22); Тест №3 (п. 5.3)	Экзаменационные билеты №9–14 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных	У1, У2, У3, У4, 31, 32, 33, 34, 35, 37, 38	Обучающийся объясняет различия OLTP и OLAP, назначение Data Lake и Data Warehouse; интерпретирует назначение ETL, ELK Stack, ClickHouse, Grafana, Kibana, Metabase, pandas; анализирует методы Data Mining, визуализации и мониторинга данных; обосновывает выбор инструментов аналитической обработки и построения дашбордов; использует средства	Реферат (п. 5.2, темы 23–30); Тест №4 (п. 5.3); Тест №5 (п. 5.3)	Экзаменационные билеты №15–30 (п. 6.1)

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС ³	
			Текущий контроль ⁴	Промежуточная аттестация ⁴
		анализа, техническую документацию и справочные системы для проектирования аналитической платформы хранения и обработки данных.		

² - для формулировки показателей использовать положения Таксономии Блума.

³ - Однотипные оценочные средства нумеруются, н-р: «Тест №2», «Контрольная работа №4».

⁴ - Примеры всех оценочных средств должны быть представлены в разделах 5,6.

⁵ - В скобках следует указать пункт разделов 5.6, в котором оно представлено.

3.2 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Раздел 1. Технологии виртуализации и автоматизации.				
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 1 Установка и базовая настройка сервера NFS в Linux: Освоение принципов работы сетевых файловых систем	У1, У2, У3, 31, 32, 37	Устанавливает и настраивает NFS-сервер, проверяет доступ клиентов, анализирует корректность работы сетевой файловой системы	Тест №1 (п. 5.3)	Практическое задание билета №1 (п. 6.1)

Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 2 Настройка SMB/CIFS-сервера и подключение клиентов: Изучение технологии совместного доступа к файлам	У1, У2, У3, 32, 37	Настраивает SMB-сервер, управляет пользователями и правами доступа, проверяет подключение клиентов	Тест №1 (п. 5.3)	Практическое задание билета №1 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 3 Сравнение производительности NFS и SMB: Анализ эффективности различных протоколов хранения	У2, У3, 37	Проводит тестирование производительности, анализирует результаты и обосновывает выбор протокола	Тест №1 (п. 5.3)	Практическое задание билета №2 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 4 Настройка сетевого хранилища с использованием iSCSI: Ознакомление с блочными протоколами доступа к данным	У1, У2, У3, 32, 37	Настраивает iSCSI target и initiator, проверяет доступ к блочным устройствам	Тест №2 (п. 5.3)	Практическое задание билета №2 (п. 6.1)

Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 5 Изучение технологии InfiniBand и её настройки в эмуляторе: Ознакомление с высокоскоростными межсоединениями	У2, 32, 37	Анализирует работу высокоскоростных интерфейсов, оценивает влияние на производительность	Тест №2 (п. 5.3)	Практическое задание билета №3 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 6 Развёртывание unified storage на базе Ceph: Практика объединения разных типов хранилищ	У1, У2, У3, 32, 37	Разворачивает распределённое хранилище, проверяет доступ и отказоустойчивость	Тест №2 (п. 5.3)	Практическое задание билета №3 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 7 Настройка программного SDS-хранилища (Software Defined Storage): Изучение программно-определяемых хранилищ	У1, У2, У3, 32, 37	Настраивает SDS-хранилище, управляет ресурсами через программные средства	Тест №2 (п. 5.3)	Практическое задание билета №3 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 8 Сравнение SDS и традиционных систем хранения: Оценка преимуществ и недостатков SDS	У2, У3, 37	Анализирует преимущества и недостатки SDS и традиционных систем	Тест №2 (п. 5.3)	Практическое задание билета №4 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 9 Развёртывание гиперконвергентной системы	У1, У2, У3, 32, 37	Разворачивает гиперконвергентную систему, проверяет работу хранилища и ВМ	Тест №2 (п. 5.3)	Практическое задание билета №4 (п. 6.1)

(Proxmox VE или TrueNAS Scale): Изучение принципов объединения хранения и вычислений				
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 10 Настройка RAID-массивов разных уровней (RAID 0/1/5/10): Освоение технологии отказоустойчивого хранения данных	У1, У2, У3, 32, 37	Настраивает RAID-массивы, проверяет отказоустойчивость	Тест №2 (п. 5.3)	Практическое задание билета №6 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 11 Исследование производительности разных уровней RAID: Практический анализ скоростей и надёжности	У2, У3, 37	Анализирует производительность RAID, делает выводы	Тест №2 (п. 5.3)	Практическое задание билета №6 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 12 Создание и подключение облачного хранилища (например, MinIO, Nextcloud): Изучение основ организации облачных хранилищ	У1, У2, У3, 32, 37	Разворачивает MinIO/Nextcloud, управляет объектами	Тест №2 (п. 5.3)	Практическое задание билета №5 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 13 Настройка эфемерных хранилищ в контейнерах: Практика временного хранения данных в облачных средах	У1, У2, 37	Настраивает временные хранилища в контейнерах	Тест №2 (п. 5.3)	Практическое задание билета №5 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных	У2, У3, 37	Настраивает мониторинг хранилищ и анализирует метрики	Тест №2 (п. 5.3)	Практическое задание билета №14

Практическое занятие № 14 Мониторинг использования хранилищ (Zabbix, Grafana): Освоение инструментов наблюдения за нагрузкой				(п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 15 Настройка политик доступа к данным в сетевом хранилище: Изучение разграничения доступа пользователей	У1, У2, 37	Настраивает права доступа и проверяет их корректность	Тест №2 (п. 5.3)	Практическое задание билета №13 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 16 Создание сценариев автоматического монтирования хранилищ: Практика автоматизации подключения ресурсов	У1, У2, 37	Настраивает автоматическое подключение хранилищ	Тест №2 (п. 5.3)	Практическое задание билета №28 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 17 Настройка и тестирование отказоустойчивости хранилища: Проверка работы при сбоях оборудования	У2, У3, 37	Проводит тестирование отказов и анализ восстановления	Тест №2 (п. 5.3)	Практическое задание билета №26 (п. 6.1)
Тема 3.1 Инфраструктура и технологии хранения данных Практическое занятие № 18 Итоговый мини-проект: развёртывание корпоративного хранилища: Комплексная интеграция всех изученных технологий	У1–У4, 31–38	Проектирует и разворачивает комплексную систему хранения	Тест №2 (п. 5.3)	Практическое задание билета №30 (п. 6.1)
Тема 3.2 Защита, репликация и	У2, У3, 37	Вычисляет контрольные суммы, выявляет изменения	Тест №3 (п. 5.3)	Практическое

миграция данных Практическое занятие № 1 Проверка целостности файлов с помощью контрольных сумм (MD5, SHA256): Изучение хеш-функций и их применения		данных, анализирует целостность файлов		задание билета №8 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 2 Настройка проверки целостности данных в хранилище (ZFS Scrub, Ceph Health): Контроль целостности в распределённых системах	У2, У3, 37	Настраивает механизмы контроля целостности, анализирует состояние хранилища	Тест №3 (п. 5.3)	Практическое задание билета №8 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 3 Настройка автоматического резервного копирования средствами rsync и cron: Освоение базовых средств резервирования	У1, У2, У3, 37	Настраивает автоматическое резервное копирование и проверяет его выполнение	Тест №3 (п. 5.3)	Практическое задание билета №9 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 4 Настройка инкрементального резервного копирования (Borg, Duplicity): Повышение эффективности хранения резервов	У2, У3, 37	Настраивает инкрементальное резервирование, анализирует эффективность хранения	Тест №3 (п. 5.3)	Практическое задание билета №9 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 5 Развёртывание системы централизованного бэкапа (например, Bacula, Veeam): Работа с корпоративными решениями резервирования	У1, У2, У3, 37	Разворачивает систему резервного копирования и управляет заданиями бэкапа	Тест №3 (п. 5.3)	Практическое задание билета №10 (п. 6.1)
Тема 3.2 Защита, репликация и	У2, У3, 37	Выполняет восстановление данных и проверяет	Тест №3 (п. 5.3)	Практическое

миграция данных Практическое занятие № 6 Тестирование восстановления данных из резервных копий: Проверка работоспособности стратегии бэкапа		корректность восстановления		задание билета №10 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 7 Настройка шифрования данных на уровне хранилища: Изучение технологий защиты при хранении	У1, У2, 37	Настраивает шифрование данных и проверяет защиту информации	Тест №3 (п. 5.3)	Практическое задание билета №27 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 8 Настройка VPN-доступа к облачному хранилищу: Практика защиты каналов связи при доступе к данным	У1, У2, 37	Настраивает защищённое соединение и проверяет доступ к хранилищу	Тест №3 (п. 5.3)	Практическое задание билета №27 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 9 Настройка политик аудита доступа к данным: Изучение журналирования действий пользователей	У2, У3, 37	Настраивает аудит действий пользователей и анализирует журналы	Тест №3 (п. 5.3)	Практическое задание билета №13 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 10 Разработка плана аварийного восстановления (Disaster Recovery Plan): Формирование стратегии восстановления инфраструктуры	У2, У3, 34, 37	Разрабатывает план восстановления системы после отказа	Тест №3 (п. 5.3)	Практическое задание билета №10 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 11 Анализ угроз и тестирование защиты облачного	У2, У3, 37	Анализирует угрозы безопасности и оценивает защищённость системы	Тест №3 (п. 5.3)	Практическое задание билета №27 (п. 6.1)

хранилища: Отработка навыков безопасности данных				
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 12 Настройка резервирования облака средствами Snapshot: Применение снимков состояния для восстановления	У1, У2, У3, 37	Настраивает snapshot и выполняет восстановление состояния системы	Тест №3 (п. 5.3)	Практическое задание билета №9 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 13 Организация геораспределённого резервного копирования: Практика распределения данных по регионам	У1, У2, У3, 37	Настраивает распределённое резервирование и проверяет синхронизацию	Тест №3 (п. 5.3)	Практическое задание билета №10 (п. 6.1)
Тема 3.2 Защита, репликация и миграция данных Практическое занятие № 14 Итоговая работа: настройка защищённой системы хранения данных: Комплексное применение средств защиты и бэкапа	У1–У4, 31–38	Разворачивает защищённую систему хранения с резервированием и контролем доступа	Тест №3 (п. 5.3)	Практическое задание билета №14 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 1 Установка и настройка PostgreSQL/MySQL как систем аналитического хранения: Освоение СУБД для хранения и анализа данных	У1, У2, У3, 32, 37	Устанавливает и настраивает СУБД, проверяет работу с данными	Тест №4 (п. 5.3)	Практическое задание билета №16 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 2 Импорт и организация структурированных данных:	У1, У2, У3, 37	Импортирует и структурирует данные для анализа	Тест №4 (п. 5.3)	Практическое задание билета №18 (п. 6.1)

Формирование аналитических наборов данных				
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 3 Использование OLAP-кубов и аналитических запросов: Изучение оперативной аналитической обработки	У2, У3, 32, 37	Выполняет аналитические запросы и интерпретирует результаты	Тест №4 (п. 5.3)	Практическое задание билета №16 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 4 Настройка инструментов ETL (Extract, Transform, Load): Практика подготовки данных для анализа	У1, У2, У3, 37	Настраивает процесс ETL и преобразует данные	Тест №4 (п. 5.3)	Практическое задание билета №18 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 5 Анализ логов и журналов хранилищ средствами ELK Stack: Освоение инструментов сбора и анализа данных	У2, У3, 37	Анализирует логи и настраивает систему сбора данных	Тест №4 (п. 5.3)	Практическое задание билета №21 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 6 Использование Power BI / Metabase для визуализации данных: Развитие навыков представления аналитики	У2, У3, 37	Строит графики и отчёты на основе данных	Тест №4 (п. 5.3)	Практическое задание билета №20 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 7 Настройка мониторинга производительности хранилищ: Анализ метрик и узких мест в	У2, У3, 37	Анализирует метрики и выявляет узкие места	Тест №4 (п. 5.3)	Практическое задание билета №29 (п. 6.1)

инфраструктуре				
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 8 Сбор и агрегация данных с разных хранилищ: Интеграция разнородных источников информации	У1, У2, У3, 37	Объединяет данные из разных источников	Тест №4 (п. 5.3)	Практическое задание билета №25 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 9 Использование Python (pandas) для анализа экспортированных данных: Автоматизация аналитических операций	У2, У3, 37	Выполняет анализ данных с использованием pandas	Тест №4 (п. 5.3)	Практическое задание билета №22 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 10 Настройка open-source хранилища данных (Hadoop / ClickHouse / MinIO): Изучение распределённых систем анализа	У1, У2, У3, 37	Настраивает аналитическое хранилище и выполняет запросы	Тест №4 (п. 5.3)	Практическое задание билета №16 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 11 Настройка политики доступа к аналитическим данным: Защита информации при аналитических операциях	У1, У2, 37	Настраивает политики доступа к аналитическим данным	Тест №5 (п. 5.3)	Практическое задание билета №13 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 12 Сравнение open-source и проприетарных аналитических систем: Анализ преимуществ и ограничений решений	У2, У3, 37	Анализирует open-source и проприетарные решения	Тест №5 (п. 5.3)	Практическое задание билета №25 (п. 6.1)

Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 13 Разработка отчётов на основе реальных данных хранилища: Практика построения отчётности	У2, У3, 37	Формирует аналитические отчёты на основе данных	Тест №5 (п. 5.3)	Практическое задание билета №24 (п. 6.1)
Тема 3.3 Анализ и интеллектуальная обработка данных Практическое занятие № 14 Итоговый проект: построение защищённой аналитической платформы: Интеграция хранения, защиты и анализа данных	У1–У4, 31–38	Разворачивает аналитическую платформу с интеграцией хранения, защиты и анализа	Тест №5 (п. 5.3)	Практическое задание билета №30 (п. 6.1)

4 Описание процедуры оценивания

Результаты обучения по дисциплине, уровень сформированности компетенций оцениваются по четырём бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом.

Критерии оценивания устного ответа

Оценочные средства: собеседование, устное сообщение

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

Оценочные средства: доклад (сообщение), в том числе выполненный в форме презентации.

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера.

Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	<i>Отлично</i>	<i>Хорошо</i>	<i>Удовлетворительно</i>	<i>Неудовлетворительно</i>
Количество правильных ответов	91 % и $\geq$	от 81% до 90,9 %	не менее 70%	менее 70%

Критерии выставления оценки студенту на зачете/ экзамене

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только

	основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

1. В чём принципиальное различие между DAS, NAS и SAN?
2. Какую роль выполняет системный администратор при организации хранилищ данных?
3. Чем отличаются протоколы NFS и SMB и в каких случаях используется каждый?
4. Как реализуется разграничение доступа в сетевых файловых системах?
5. Какие основные угрозы безопасности существуют при работе с файловыми протоколами?
6. Что такое InfiniBand и где он применяется?
7. Какие преимущества даёт использование высокоскоростных интерфейсов в дата-центрах?
8. Что такое Unified Storage и какие задачи он решает?
9. В чём отличие SDS (Software Defined Storage) от традиционных хранилищ?
10. Какие преимущества даёт управление хранилищем через API?
11. Что такое гиперконвергентная инфраструктура (HCI) и как она работает?
12. В чём отличие VMware vSAN от классических SAN решений?
13. Что такое облачное хранилище и чем оно отличается от локального?
14. Что такое S3-хранилище и как устроена его модель данных?
15. Что такое эфемерные (ephemeral) хранилища и где они применяются?
16. Какие уровни RAID существуют и в чём их различия?
17. В чём разница между аппаратным и программным RAID?
18. Какие open-source системы хранения ты знаешь и чем они отличаются?
19. Чем Ceph отличается от GlusterFS?
20. Какие преимущества у проприетарных решений (Dell EMC, NetApp) по сравнению с open-source?
21. Как проверяется целостность данных и какие алгоритмы для этого используются?
22. В чём разница между MD5 и SHA256 и где их применяют?
23. Что такое контроль версий данных в S3-хранилищах?
24. Какие существуют виды резервного копирования и чем они отличаются?
25. Что такое snapshot и как он используется для восстановления данных?
26. Как работает репликация данных и чем отличается от резервного копирования?
27. Какие инструменты используются для миграции данных между системами?
28. Что такое дедупликация данных и какие преимущества она даёт?
29. Как реализуется контроль доступа (ACL, POSIX, IAM) в системах хранения?
30. Какие инструменты используются для мониторинга и диагностики хранилищ?

5.2 Темы рефератов

1. Архитектурные подходы к построению систем хранения данных в современных ИТ-инфраструктурах
2. Организация сетевых файловых сервисов в корпоративной среде
3. Практические аспекты обеспечения безопасности при работе с сетевыми протоколами хранения данных
4. Высокоскоростные межсоединения в дата-центрах: роль и значение InfiniBand
5. Интеграция файловых и блочных хранилищ в рамках концепции Unified Storage
6. Эволюция систем хранения: переход от традиционных решений к SDS
7. Управление хранилищами через API как основа автоматизации инфраструктуры
8. Архитектура и применение гиперконвергентных инфраструктур в бизнесе
9. Сравнение локальных и облачных моделей хранения данных
10. Объектные хранилища и их роль в современных облачных сервисах
11. Использование эфемерных хранилищ в контейнеризированных средах
12. Обеспечение отказоустойчивости с использованием RAID-технологий
13. Сравнительный анализ open-source систем хранения данных
14. Проприетарные решения в области хранения данных и их место в корпоративной инфраструктуре
15. Методы контроля целостности данных в распределённых системах хранения
16. Хеширование как инструмент обеспечения надёжности и контроля данных
17. Репликация и резервирование как ключевые механизмы защиты данных
18. Стратегии резервного копирования в облачных средах
19. Миграция данных между различными инфраструктурами: подходы и инструменты
20. Оптимизация хранения данных с использованием дедупликации и сжатия
21. Организация контроля доступа и аудита в системах хранения данных
22. Мониторинг и диагностика производительности систем хранения
23. Архитектура аналитических систем: различие OLTP и OLAP подходов
24. Data Lake и Data Warehouse как основы аналитической инфраструктуры
25. Применение OLAP-кубов для многомерного анализа данных
26. Методы интеллектуального анализа данных в современных системах
27. ETL-процессы как основа интеграции данных
28. Облачные платформы аналитики и их применение в бизнесе
29. Инструменты визуализации и анализа данных в ИТ-инфраструктуре
30. Комплексная архитектура хранения, защиты и анализа данных в корпоративных системах

5.3 Примеры тестовых заданий

Тест №1

1. Какое ключевое отличие SAN от NAS влияет на уровень взаимодействия с файловой системой?
 - а) SAN использует файловый доступ на уровне ОС
 - б) NAS работает на блочном уровне
 - в) SAN предоставляет блочный доступ к устройствам (верно)
 - г) NAS не использует сетевые протоколы
2. Какой фактор наиболее критичен при выборе между NFS и SMB в Linux-среде?
 - а) Поддержка POSIX-прав доступа (верно)
 - б) Использование TCP вместо UDP
 - в) Наличие GUI для администрирования

г) Скорость работы DNS

3. Что является особенностью InfiniBand по сравнению с Ethernet?

- а) Работа исключительно на уровне IP
- б) Использование RDMA для прямого доступа к памяти (верно)
- в) Отсутствие маршрутизации
- г) Ограничение скорости до 10 Гбит/с

4. Что характеризует Unified Storage?

- а) Использование только объектного хранения
- б) Разделение файлового и блочного доступа
- в) Объединение различных типов доступа к данным (верно)
- г) Работа исключительно в облаке

5. Какой принцип лежит в основе SDS?

- а) Привязка к аппаратному RAID
- б) Управление через гипервизор
- в) Абстракция хранения от аппаратного уровня (верно)
- г) Использование исключительно SSD

6. Что является отличительной чертой HCI?

- а) Отдельное масштабирование сетей
- б) Интеграция вычислений и хранения в одном узле (верно)
- в) Использование только SAN
- г) Отсутствие виртуализации

7. Что характерно для S3-хранилищ?

- а) Фиксированная структура каталогов
- б) Объектная модель с уникальными ключами (верно)
- в) Работа только по протоколу FTP
- г) Прямая работа с блочными устройствами

8. Какой RAID обеспечивает баланс между отказоустойчивостью и производительностью?

- а) RAID 0
- б) RAID 1
- в) RAID 5 (верно)
- г) RAID 0+0

9. Что отличает Ceph от классических SAN?

- а) Отсутствие масштабируемости
- б) Централизованное управление дисками
- в) Распределённая архитектура хранения (верно)
- г) Работа только с SSD

10. Какое преимущество проприетарных решений наиболее значимо?

- а) Полное отсутствие лицензий
- б) Минимальная стоимость
- в) Интеграция и поддержка от вендора (верно)
- г) Отсутствие документации

Время выполнения – 10 минут

Тест №2

1. При настройке NFS, что определяет доступ клиентов?
 - а) /etc/passwd
 - б) /etc/exports (верно)
 - в) /etc/network
 - г) /etc/fstab

2. Что является особенностью SMB?
 - а) Работа только в Linux
 - б) Интеграция с доменной аутентификацией (верно)
 - в) Отсутствие прав доступа
 - г) Использование UDP

3. Что является преимуществом iSCSI?
 - а) Работа без сети
 - б) Использование IP-сетей для блочного доступа (верно)
 - в) Работа только с файлами
 - г) Отсутствие адресации

4. Что даёт использование Ceph в unified storage?
 - а) Только файловое хранение
 - б) Только блочное хранение
 - в) Поддержку разных типов доступа (верно)
 - г) Ограничение масштабируемости

5. Что является ключевой особенностью Proxmox VE в HCI?
 - а) Отсутствие виртуализации
 - б) Интеграция хранения и виртуализации (верно)
 - в) Работа только с Windows
 - г) Поддержка только RAID 0

6. Что влияет на производительность RAID?
 - а) Только объём дисков
 - б) Тип RAID и количество дисков (верно)
 - в) Цвет кабелей
 - г) Версия BIOS

7. Что измеряется при сравнении NFS и SMB?
 - а) Только задержка сети
 - б) Производительность и нагрузка (верно)
 - в) Количество пользователей
 - г) Версия ОС

8. Что характерно для ephemeral storage?
 - а) Долговременное хранение
 - б) Удаление данных при завершении сессии (верно)
 - в) Резервное копирование
 - г) Работа только с RAID

9. Что делает мониторинг (Zabbix/Grafana)?

- а) Управляет RAID
- б) Отслеживает метрики системы (верно)
- в) Удаляет данные
- г) Настраивает сеть

10. Что обеспечивает автоматическое монтирование?

- а) DHCP
- б) fstab или скрипты (верно)
- в) BIOS
- г) RAID

Время выполнения – 10 минут

Тест №3

1. Что означает контроль целостности данных?

- а) Сжатие данных
- б) Проверка неизменности данных (верно)
- в) Удаление дубликатов
- г) Шифрование

2. Что является слабостью MD5?

- а) Медленная работа
- б) Коллизии хешей (верно)
- в) Сложность реализации
- г) Большой размер

3. Что даёт snapshot?

- а) Удаление данных
- б) Состояние системы на момент времени (верно)
- в) Сжатие данных
- г) Репликацию

4. Что отличает инкрементальный бэкап?

- а) Копирует всё
- б) Копирует только изменения после последнего бэкапа (верно)
- в) Удаляет старые данные
- г) Не требует хранения

5. Что делает rsync?

- а) Шифрует данные
- б) Синхронизирует изменения файлов (верно)
- в) Форматирует диск
- г) Управляет RAID

6. Что такое георепликация?

- а) Копирование на один диск
- б) Распределение данных между регионами (верно)
- в) Архивация
- г) Шифрование

7. Что даёт дедупликация?

- а) Ускорение сети
- б) Удаление повторяющихся данных (верно)
- в) Шифрование
- г) Удаление файлов

8. Что определяет ACL?

- а) Скорость доступа
- б) Права доступа пользователей (верно)
- в) Размер файлов
- г) Тип RAID

9. Что делает IAM в облаке?

- а) Управляет дисками
- б) Управляет доступом и ролями (верно)
- в) Ускоряет сеть
- г) Удаляет данные

10. Что включает Disaster Recovery Plan?

- а) Только бэкап
- б) План восстановления после сбоев (верно)
- в) Настройку RAID
- г) Мониторинг

Время выполнения – 10 минут

Тест №4

1. Чем OLAP отличается от OLTP?

- а) OLTP быстрее
- б) OLAP используется для анализа данных (верно)
- в) OLAP не хранит данные
- г) OLTP не использует SQL

2. Что характерно для Data Lake?

- а) Строгая структура
- б) Хранение сырых данных (верно)
- в) Только SQL
- г) Только таблицы

3. Что такое OLAP-куб?

- а) База данных
- б) Многомерная модель данных (верно)
- в) RAID
- г) API

4. Что делает ETL?

- а) Удаляет данные
- б) Извлекает, преобразует и загружает данные (верно)
- в) Шифрует
- г) Реплицирует

5. Что используется для визуализации?

- а) Bash
- б) Grafana (верно)
- в) BIOS
- г) RAID

6. Что делает ELK Stack?

- а) Управляет RAID
- б) Анализирует и хранит логи (верно)
- в) Шифрует
- г) Удаляет данные

7. Что делает pandas?

- а) Управляет сетью
- б) Анализирует данные (верно)
- в) Устанавливает ОС
- г) Управляет RAID

8. Что такое Data Mining?

- а) Удаление данных
- б) Поиск закономерностей (верно)
- в) Сжатие
- г) Хеширование

9. Что делает ClickHouse?

- а) OLTP
- б) Аналитические запросы (верно)
- в) RAID
- г) Backup

10. Что делает Kibana?

- а) Хранит данные
- б) Визуализирует данные (верно)
- в) Шифрует
- г) Удаляет

Время выполнения – 10 минут

Тест №5

1. Что объединяет хранение, защиту и анализ данных?

- а) RAID
- б) Архитектура системы (верно)
- в) BIOS
- г) DNS

2. Что важно при построении хранилища?

- а) Только объём
- б) Надёжность и масштабируемость (верно)
- в) Цвет серверов
- г) ОС

3. Что влияет на отказоустойчивость?

- а) RAID и репликация (верно)
- б) DNS
- в) GUI
- г) CPU

4. Что даёт мониторинг?

- а) Удаление ошибок
- б) Выявление проблем (верно)
- в) Шифрование
- г) RAID

5. Что важно при миграции данных?

- а) Только скорость
- б) Целостность и совместимость (верно)
- в) Цвет кабеля
- г) BIOS

6. Что даёт автоматизация?

- а) Усложнение
- б) Повышение эффективности (верно)
- в) Удаление данных
- г) RAID

7. Что важно в аналитике?

- а) Размер диска
- б) Качество данных (верно)
- в) BIOS
- г) RAID

8. Что влияет на производительность?

- а) Архитектура системы (верно)
- б) Цвет интерфейса
- в) DNS
- г) Пользователь

9. Что важно при безопасности?

- а) RAID
- б) Контроль доступа и шифрование (верно)
- в) BIOS
- г) CPU

10. Что определяет эффективность системы?

- а) Только скорость
- б) Баланс параметров (надёжность, скорость, масштабируемость) (верно)
- в) Цвет оборудования
- г) GUI

Время выполнения – 10 минут

6. Примеры оценочных средств для проведения промежуточной аттестации

6.1 Варианты экзаменационных билетов:

Экзаменационный билет №1

1. Сравните архитектуры DAS, NAS и SAN с точки зрения уровня доступа (блочный/файловый), масштабируемости, отказоустойчивости и сценариев применения в корпоративной инфраструктуре.
2. Проанализируйте особенности реализации разграничения доступа и механизмов безопасности в NFS и SMB, включая модели аутентификации и управления правами.

Практическое задание:

На Linux-сервере настроить NFS: создать каталог /srv/share, настроить экспорт через /etc/exports с доступом для двух клиентов (один read-only, второй read-write), смонтировать ресурс на клиентах и подтвердить различие прав через запись/чтение файлов.

Экзаменационный билет №2

1. Раскройте принципы работы InfiniBand, включая RDMA, и объясните его преимущества для высоконагруженных систем.
2. Охарактеризуйте архитектуру Unified Storage и механизм одновременной работы с файловыми и блочными протоколами.

Практическое задание:

Разработать схему инфраструктуры хранения для офиса (30 пользователей): файловый доступ (SMB), блочный доступ (iSCSI для БД). Указать: серверы, сеть, протоколы, точки отказа и способ резервирования.

Экзаменационный билет №3

1. Подробно объясните концепцию Software Defined Storage, включая абстракцию ресурсов и управление через API.
2. Разберите архитектуру Ceph (MON, OSD, MDS) и механизм размещения данных.

Практическое задание:

Развернуть MinIO: создать bucket “data”, включить доступ через access key/secret key, загрузить 3 файла через CLI (mc или aws-cli), проверить доступность объектов.

Экзаменационный билет №4

1. Объясните архитектуру гиперконвергентных систем и их отличие от классической трёхуровневой архитектуры.
2. Сравните VMware vSAN и классические SAN по управлению и масштабированию.

Практическое задание:

В Proxmox создать виртуальную машину, подключить к ней локальное хранилище (directory storage), создать диск VM и проверить запись/чтение данных внутри VM.

Экзаменационный билет №5

1. Проанализируйте модели облачных хранилищ (объектное, файловое, блочное) и области их применения.
2. Объясните модель S3 (bucket, object, key, versioning).

Практическое задание:

В MinIO включить versioning для bucket, загрузить файл, изменить его и загрузить снова, затем через CLI восстановить первую версию.

Экзаменационный билет №6

1. Объясните принципы RAID 0,1,5,10 и различия в отказоустойчивости.

2. Сравните программный и аппаратный RAID.

Практическое задание:

Создать RAID 1 через mdadm из двух дисков, смонтировать в /mnt/raid, записать файл, отключить один диск (simulate fail) и проверить доступность данных.

Экзаменационный билет №7

1. Сравните Ceph, GlusterFS и TrueNAS по архитектуре и масштабируемости.

2. Проанализируйте преимущества проприетарных решений (NetApp, Dell EMC).

Практическое задание:

Составить таблицу сравнения (минимум 6 критериев: масштабируемость, отказоустойчивость, тип доступа, сложность настройки, стоимость, производительность).

Экзаменационный билет №8

1. Объясните методы контроля целостности данных (CRC, хеширование).

2. Сравните MD5 и SHA256 с точки зрения безопасности.

Практическое задание:

Создать файл, вычислить md5sum и sha256sum, изменить файл (добавить строку) и доказать изменение через повторный расчёт.

Экзаменационный билет №9

1. Объясните принцип snapshot и отличие от полного бэкапа.

2. Сравните инкрементальный и дифференциальный бэкап.

Практическое задание:

Настроить резервное копирование каталога /data в /backup через rsync с ключом –delete, добавить стоп-задачу на выполнение каждые 5 минут и проверить лог выполнения.

Экзаменационный билет №10

1. Раскройте синхронную и асинхронную репликацию.

2. Объясните георепликацию и её применение.

Практическое задание:

Настроить синхронизацию двух каталогов на разных машинах через rsync по SSH, выполнить изменение файла и проверить его появление на второй машине.

Экзаменационный билет №11

1. Объясните процессы миграции данных между локальными и облачными хранилищами.

2. Сравните rsync и rclone.

Практическое задание:

С помощью rclone скопировать каталог в MinIO (или S3-совместимое хранилище), проверить структуру и целостность файлов.

Экзаменационный билет №12

1. Объясните дедупликацию и её влияние на хранение данных.

2. Проанализируйте методы сжатия.

Практическое задание:

Создать каталог с повторяющимися файлами, заархивировать его (tar.gz), сравнить размер до и после, сделать вывод об эффективности.

Экзаменационный билет №13

1. Объясните модели контроля доступа (POSIX, ACL, IAM).

2. Проанализируйте аудит доступа.

Практическое задание:

Создать 3 пользователей, назначить им разные права (чтение/запись/запрет) к одному каталогу и проверить доступ под каждым пользователем.

Экзаменационный билет №14

1. Объясните архитектуру мониторинга (Zabbix/Prometheus).
2. Проанализируйте ключевые метрики хранения (IOPS, latency, throughput).

Практическое задание:

С помощью iostat или dstat снять метрики диска при копировании большого файла (>1 ГБ), зафиксировать значения и сделать вывод о нагрузке.

Экзаменационный билет №15

1. Объясните различия OLTP и OLAP.
2. Сравните Data Lake и Data Warehouse.

Практическое задание:

Разработать схему: источник данных (логи), хранилище (Data Lake), аналитика (OLAP), указать потоки данных.

Экзаменационный билет №16

1. Объясните OLAP-кубы и многомерный анализ.
2. Охарактеризуйте ClickHouse.

Практическое задание:

Создать таблицу (дата, продукт, продажи), выполнить запрос SUM продаж по продукту и дате.

Экзаменационный билет №17

1. Объясните методы Data Mining (кластеризация, классификация).
2. Проанализируйте задачи прогнозирования.

Практическое задание:

В Excel или Python разбить данные (например, продажи) по группам и определить тренд (рост/падение).

Экзаменационный билет №18

1. Подробно опишите ETL-процесс.
2. Сравните Airbyte и NiFi.

Практическое задание:

Взять CSV-файл, изменить структуру (переименовать столбцы, удалить лишние), загрузить в БД (SQLite/MySQL).

Экзаменационный билет №19

1. Объясните архитектуру облачных аналитических платформ.
2. Сравните BigQuery и Athena.

Практическое задание:

Составить SQL-запрос: подсчитать количество записей и среднее значение по колонке в таблице.

Экзаменационный билет №20

1. Объясните принципы визуализации данных.
2. Сравните Grafana, Kibana и Metabase.

Практическое задание:

Построить 3 графика (CPU, диск, сеть) в Grafana или аналоге на основе собранных метрик.

Экзаменационный билет №21

1. Объясните архитектуру ELK Stack.
2. Проанализируйте сбор логов (Fluentd, Loki).

Практическое задание:

Настроить сбор логов (например, system logs) и вывести их в интерфейсе (Kibana/Grafana Loki).

Экзаменационный билет №22

1. Объясните применение Python в анализе данных.
2. Охарактеризуйте pandas.

Практическое задание:

Загрузить CSV в pandas, вывести среднее значение по столбцу и сгруппировать данные.

Экзаменационный билет №23

1. Объясните применение ML для анализа логов.
2. Проанализируйте методы обнаружения аномалий.

Практическое задание:

На основе логов (время ответа) определить выбросы (значения выше среднего в 2 раза).

Экзаменационный билет №24

1. Объясните принципы построения дашбордов.
2. Проанализируйте метрики хранения.

Практическое задание:

Составить список метрик (минимум 5: CPU, RAM, IOPS, latency, disk usage) и описать, какие графики нужны.

Экзаменационный билет №25

1. Объясните интеграцию хранения, защиты и анализа данных.
2. Охарактеризуйте архитектуру корпоративной системы.

Практическое задание:

Спроектировать систему: файловое хранилище + бэкап + аналитика логов. Указать компоненты и связи.

Экзаменационный билет №26

1. Объясните механизмы отказоустойчивости (RAID, репликация).
2. Проанализируйте тестирование отказов.

Практическое задание:

Смоделировать отказ диска (удалить диск из RAID), проверить состояние массива и восстановить его.

Экзаменационный билет №27

1. Объясните методы защиты данных (шифрование, VPN).
2. Проанализируйте угрозы хранения данных.

Практическое задание:

Зашифровать каталог с помощью openssl или gpg и проверить доступ к данным.

Экзаменационный билет №28

1. Объясните автоматизацию работы с хранилищами.
2. Проанализируйте использование cron и скриптов.

Практическое задание:

Создать bash-скрипт: монтирование ресурса + резервное копирование + логирование.

Экзаменационный билет №29

1. Объясните анализ производительности систем хранения.
2. Проанализируйте выявление узких мест.

Практическое задание:

С помощью dd или fio провести тест записи/чтения, измерить скорость и сделать вывод.

Экзаменационный билет №30

1. Объясните комплексную архитектуру хранения, защиты и анализа данных.
2. Проанализируйте взаимодействие компонентов системы.

Практическое задание:

Разработать проект: 1 сервер хранения (NFS), 1 сервер бэкапа (rsync), 1 сервер мониторинга (Grafana). Описать взаимодействие и схему.