МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.03.02 Безопасность облачных сервисов

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2026

Рабочая программа МДК.03.02 Безопасность облачных сервисов профессионального модуля ПМ.03 Эксплуатация 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 № 9__ от «_18__» ___05____2026_ г.

Председатель ЦМК _____ *Е.А. Стефанович*
подпись

Согласована:

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

_____ *Д.М. Шумов*
(подпись, печать)

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина МДК.03.02 Безопасность облачных сервисов является частью профессионального цикла основной образовательной программы (далее ООП) в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

1.2 Цель и планируемые результаты освоения дисциплины

По итогам освоения дисциплины, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице.

Код компетенции	Умения	Знания
ПК 3.5	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	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
ПК 3.6	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	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами; важность и назначение сетевого траффика, 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

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	170
в том числе:	
– теоретическое обучение	46
– практические занятия	74
– курсовая проект	0
– самостоятельная работа	46
– консультации	2
– промежуточная аттестация – экзамен	4

2.2 Тематический план и содержание учебной дисциплины

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 2. Безопасность облачных сервисов			**120/74**
МДК.03.02. Безопасность облачных сервисов			**120/74**
Тема 2.1. Основы и архитектура безопасности облачных сервисов	**Содержание**		**14**
	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	
	5	**Архитектура облачной безопасности** Защита данных, сетей, пользователей, приложений	
	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		**24**
	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	**Содержание**		**16**

устойчивость инфраструктуры	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	
	6	**Централизованный сбор логов** ELK, Grafana Loki, аудит событий	
	7	**Резервное копирование и восстановление данных** Snapshot, репликация, Disaster Recovery	
	8	**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 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.			**46**

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**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Материально-техническое обеспечение

Для реализации программы учебной дисциплины предусмотрено наличие следующих специальных помещений:

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 учебной дисциплины библиотечный фонд ВВГУ укомплектован печатными и электронными изданиями.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Основная литература

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
У1 – разрабатывать и внедрять процессы проверки подлинности на уровне подразделения и компании в целом, контролировать доступ к системе управления общедоступным облаком	- правильность выполнения практических работ; - правильность, полнота самостоятельной подготовки к выполнению заданий по практическим работам	устный опрос; оценка выполнения и защиты практических работ.
У2 – использовать общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости	- правильность выполнения практических работ; - правильность, полнота самостоятельной подготовки к выполнению заданий по практическим работам	устный опрос; оценка выполнения и защиты практических работ.
У3 – проводить постоянные проверки отказоустойчивости и восстановления системы	- правильность выполнения практических работ; - правильность, полнота самостоятельной подготовки к выполнению заданий по практическим работам	устный опрос; оценка выполнения и защиты практических работ.
У4 – внедрение решений для мониторинга с целью формирования предупреждений и автоматизации реагирования на различные инциденты	- правильность выполнения практических работ; - правильность, полнота самостоятельной подготовки к выполнению заданий по практическим работам	устный опрос; оценка выполнения и защиты практических работ.
У5 – поддерживать облачные конфигурации в актуальном	- правильность выполнения практических работ;	устный опрос; оценка выполнения и

состоянии и вести учет контроля версий	- правильность, полнота самостоятельной подготовки к выполнению заданий по практическим работам	защиты практических работ.
У6 – внедрять централизованный сбор и анализ метрик для системной, сетевой и прикладной информации	- правильность выполнения практических работ; - правильность, полнота самостоятельной подготовки к выполнению заданий по практическим работам	устный опрос; оценка выполнения и защиты практических работ.
У7 – проводить постоянные проверки отказоустойчивости и восстановления системы	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З1 – методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З2 – важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З3 – требования к совместимости компонентов внутри облачной инфраструктуры	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З4 – методики и возможности автоматизации, широко используемые в техническом сообществе	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З5 – сетевой поток данных и соответствующая зависимость доступности систем	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.

З6 – требования к производительности и возможные узкие места при проектировании инфраструктуры	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З7 – различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З8 – важность и назначение сетевого траффика, а также изоляцию ресурсов	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З9 – различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З10 – сетевой поток данных и соответствующая зависимость доступности систем	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З11 – как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.
З12 – требования к производительности и возможные узкие места при проектировании инфраструктуры	- четкость изложения материала при устном опросе; - правильность выполнения теста - правильность, полнота самостоятельной подготовки к устному опросу и зачету	- устный опрос; - оценка выполнения и защиты практических работ.

Для оценки достижения запланированных результатов обучения по дисциплине разработаны контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации, которые прилагаются к рабочей программе дисциплины.

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 2026

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 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.03.02 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	З1	методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам
ПК 3.5	З2	важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений
ПК 3.5	З3	требования к совместимости компонентов внутри облачной инфраструктуры
ПК 3.5	З4	методики и возможности автоматизации, широко используемые в техническом сообществе
ПК 3.5	З5	сетевой поток данных и соответствующая зависимость доступности систем
ПК 3.5	З6	требования к производительности и возможные узкие места при проектировании инфраструктуры
ПК 3.6	З7	различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами
ПК 3.6	З8	важность и назначение сетевого траффика, а также изоляцию ресурсов
ПК 3.6	З9	различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками
ПК 3.6	З10	сетевой поток данных и соответствующая зависимость доступности систем
ПК 3.6	З11	как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур
ПК 3.6	З12	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, З1, З2, З3, З4, З5, З6	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, З5, З6, З7, З8, З9, З10, З11, З12	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 траффика, 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, З1, З4, З7, З8, З9, З10, З11, З12	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 траффика, 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 № 1Модели облачных сервисов: Анализ IaaS, PaaS, SaaS. Определение зон ответственности	У1, З1, З2	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, З3, З6	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, З4	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, З2, З4	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, З5, З6	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, З5	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, З1, З2, З6	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, З6	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, З5	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, З1, З6	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, З7, З8	Внедряет централизованный сбор и анализ метрик, использует различные сетевые архитектуры и изоляцию 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, З8	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, З10	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, З11	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 устойчивость инфраструктуры Практическое занятие № 5 Централизованный сбор логов: Настройка ELK или Grafana Loki	У6, З11	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 устойчивость инфраструктуры Практическое занятие № 6 Анализ журналов безопасности: Выявление подозрительных событий	У4, З11	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 устойчивость инфраструктуры Практическое занятие № 7 Настройка защиты от DoS/DDoS: Rate limiting, Fail2Ban, Cloudflare	У4, З9	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 устойчивость инфраструктуры Практическое занятие № 8 Настройка резервного копирования: Репликация данных, инкрементальные бэкапы	У7, З12	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 устойчивость инфраструктуры Практическое занятие № 9 Настройка высокой доступности: HAProxy, Keepalived, балансировка нагрузки	У7, З9	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 устойчивость инфраструктуры	У7, З12	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, З11	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, З11	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, З1	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, З3	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, З2	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, З4	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, З6	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, З6	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, З6	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, З1	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, З11	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, З1	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, З1	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, З1	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 четырёх 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	*Отлично*	*Хорошо*	*Удовлетворительно*	*Неудовлетворительно*
Количество правильных ответов	91 % и ≥	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:
Продемонстрировать 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.