ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

C=RU, S=Ставропольский край, L=г. Ставрополь, T=проректор по учебной работе, OU=ректорат, O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "" СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ""", СНИЛС=15230589951, ИНН=263411176761, E=s.a.maksimovich@stgau.ru, G=Светлана Александровна, SN=Максимович, CN=Максимович Светлана Александровна

УТВЕРЖДАЮ

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

_____

_____

«___» _____ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

ФТД.01 Безопасность облачных технологий

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

очная

Ставрополь, 2026

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения	Перечень планируемых результатов обучения по дисциплине
ПК-4 Способен администрировать средства защиты информации и обеспечивать безопасность информационных систем	ПК-4.1 Администрирует средства защиты информации прикладного и системного программного обеспечения (ОС, СУБД, приложения), настраивая политики безопасности и контролируя их соблюдение	**знает** архитектуру облачных сервисов, методы защиты ОС/СУБД/приложений в облаке, политики безопасности и инструменты мониторинга их соблюдения
		умеет администрировать средства защиты, настраивать политики безопасности (IAM, сетевые, шифрования), контролировать их соблюдение и устранять отклонения
		владеет навыками навыками настройки политик безопасности в облачных средах, контроля соблюдения, выявления и устранения нарушений, документирования
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. Вырабатывает сратегию действий	**знает** системные принципы организации облачных сред и классификацию угроз для облачных технологий
		умеет идентифицировать составляющие проблемной ситуации в облачной среде и вырабатывать стратегию действий
		владеет навыками навыками системного анализа проблемных ситуаций и выработки стратегических решений для защиты облачных сред
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной	**знает** источники информации по безопасности облачных технологий, типовые алгоритмы решения задач и структуру их декомпозиции
		умеет находить и анализировать информацию, определять задачи для разработки и предлагать способы их решения

	ситуации на основе источников информации. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей разработке. Предлагает способы их решений	**владеет навыками** навыками поиска и систематизации информации, декомпозиции задач и выработки конкретных решений для облачной безопасности

2. Перечень оценочных средств по дисциплине

№	Наименование раздела/темы	Семестр	Код индикаторов достижения компетенций	Оценочное средство проверки результатов достижения индикаторов компетенций
1.	1 раздел. Безопасность облачных технологий			
1.1.	МОДУЛЬ 1. Основы безопасности облачных инфраструктур	1		Устный опрос
1.2.	МОДУЛЬ 2. Управление доступом, защита данных и применение ИИ для мониторинга	1		Задачи
1.3.	КТ 1	1		Тест
1.4.	МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред	1		Задачи
1.5.	КТ 2	1		Тест
1.6.	Зачет	1		Тест
	Промежуточная аттестация			За

3. Оценочные средства (оценочные материалы)

Примерный перечень оценочных средств для текущего контроля успеваемости и промежуточной аттестации

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде (Оценочные материалы)
Текущий контроль			
	Для оценки знаний		

1	Устный опрос	Средство контроля знаний студентов, способствующее установлению непосредственного контакта между преподавателем и студентом, в процессе которого преподаватель получает широкие возможности для изучения индивидуальных особенностей усвоения студентами учебного материала.	Перечень вопросов для устного опроса
2	Задачи	Задачи репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и правильное использование специальных терминов и понятий, узнавание объектов изучения в рамках определенного раздела дисциплины;	Комплект задач минимального уровня
3	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
	Для оценки умений		
	Для оценки навыков		
	Промежуточная аттестация		
4	Зачет	Средство контроля усвоения учебного материала практических и семинарских занятий, успешного прохождения практик и выполнения в процессе этих практик всех учебных поручений в соответствии с утвержденной программой с выставлением оценки в виде «зачтено», «незачтено».	Перечень вопросов к зачету

4. Примерный фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) "Безопасность облачных технологий"

Примерные оценочные материалы для текущего контроля успеваемости

ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ
«Безопасность облачных технологий»
МОДУЛЬ 1. Основы безопасности облачных инфраструктур
Форма: Одиночный выбор (1–10)

1. Какая модель облачного сервиса предоставляет пользователю максимальный контроль над инфраструктурой?

A) SaaS

B) PaaS

C) IaaS

D) FaaS

Правильный ответ: C

2. Какая модель развертывания облака предполагает использование инфраструктуры, принадлежащей одной организации и недоступной для внешних пользователей?

A) Публичное облако

B) Частное облако

C) Гибридное облако

D) Мультиоблако

Правильный ответ: B

3. Кто отвечает за безопасность гипервизора в модели IaaS согласно Shared Responsibility Model?

A) Клиент (потребитель облачных услуг)

B) Провайдер облачных услуг

C) Регулятор

D) Сторонний аудитор

Правильный ответ: B

4. Что из перечисленного НЕ является угрозой для облачных сред?

A) Несанкционированный доступ к данным

B) Отказ в обслуживании (DDoS)

C) Прямое физическое подключение к серверу злоумышленником

D) Уязвимости в API управления

Правильный ответ: C

5. Какой нормативный акт РФ регулирует обработку персональных данных в облачных средах?

A) ФЗ-149 «Об информации»

B) ФЗ-152 «О персональных данных»

C) ФЗ-187 «О безопасности КИИ»

D) Приказ ФСТЭК №31

Правильный ответ: B

6. Что такое мультиоблако (multi-cloud)?

A) Использование нескольких центров обработки данных одного провайдера

B) Использование сервисов нескольких облачных провайдеров одновременно

C) Сочетание публичного и частного облака

D) Облачная среда с несколькими арендаторами

Правильный ответ: B

7. Какое требование к облачным провайдерам предъявляет ФЗ-152 для обработки персональных данных?

A) Обязательное использование только российских провайдеров

B) Хранение баз данных на территории РФ

C) Использование исключительно IaaS-модели

D) Отказ от использования шифрования

Правильный ответ: B

8. Кто несёт ответственность за безопасность прикладного ПО, развёрнутого на виртуальной машине в IaaS?

A) Провайдер

B) Клиент

C) Совместно

D) Производитель ПО

Правильный ответ: B

9. Что из перечисленного относится к физическим мерам безопасности облачных дата-центров?

A) Шифрование данных

B) Система контроля доступа (биометрия)

C) Антивирусная защита виртуальных машин

D) Настройка IAM-политик

Правильный ответ: B

10. Какая модель облачного сервиса позволяет запускать код без управления серверами и кластерами?

A) IaaS

B) PaaS

C) SaaS

D) FaaS

Правильный ответ: D

Форма: Множественный выбор (11–14)
11. Какие компоненты входят в облачную инфраструктуру? (Выберите все верные)

A) Виртуальные машины

B) Объектное хранилище

C) Физические серверы

D) Сетевые коммутаторы

Правильные ответы: A, B, C, D

12. Какие модели развёртывания облачных сред существуют? (Выберите все верные)

A) Публичное облако

B) Частное облако

C) Гибридное облако

D) Выделенное облако

Правильные ответы: A, B, C

13. Какие из перечисленных угроз характерны для облачных сред? (Выберите все верные)

A) Утечка данных из-за ошибок конфигурации

B) Несанкционированный доступ через IAM

C) Физический доступ к серверу злоумышленником в дата-центре

D) DDoS-атака

Правильные ответы: A, B, D

14. Какие требования предъявляются к облачным провайдерам для работы с персональными данными в РФ? (Выберите все верные)

A) Локализация баз данных на территории РФ

B) Уведомление Роскомнадзора о начале обработки

C) Использование только российского ПО

D) Обеспечение шифрования данных

Правильные ответы: A, B, D

Форма: Сопоставление (15–17)
15. Установите соответствие между моделью облачного сервиса и её характеристикой:

Модель Характеристика
1. IaaS A. Полный контроль над инфраструктурой
2. PaaS B. Среда разработки и развертывания приложений
3. SaaS C. Готовое приложение, доступное через браузер
4. FaaS D. Выполнение кода в ответ на события
Правильный ответ:

1 → A

2 → B

3 → C

4 → D

16. Установите соответствие между понятием и его определением:

Понятие Определение
1. IAM A. Управление идентификацией и доступом
2. KMS B. Система управления ключами шифрования
3. SIEM C. Информационная система управления событиями безопасности
4. CSPM D. Управление состоянием безопасности облачных сред
Правильный ответ:

1 → A

2 → B

3 → C

4 → D

17. Установите соответствие между компонентом облачной безопасности и его функцией:

Компонент Функция
1. Security Groups A. Правила фильтрации трафика на уровне виртуальной машины
2. IAM Policies B. Определение разрешений для пользователей и сервисов
3. KMS C. Управление ключами шифрования
4. CloudTrail D. Аудит действий пользователей и сервисов
Правильный ответ:

1 → A

2 → B

3 → C

4 → D

Форма: Последовательность (18–19)
18. Расположите этапы облачной миграции в правильной последовательности:

Тестирование в облачной среде

Миграция данных и приложений

Оценка и планирование миграции

Оптимизация и мониторинг

Правильный ответ: 3 → 2 → 1 → 4

19. Расположите уровни ответственности в модели Shared Responsibility для IaaS от провайдера к клиенту:

Безопасность приложений и кода

Физическая безопасность дата-центра

Безопасность гостевой ОС и ПО

Безопасность гипервизора

Правильный ответ: 2 → 4 → 3 → 1

МОДУЛЬ 2. Управление доступом, защита данных и ИИ-мониторинг
Форма: Одиночный выбор (20–24)
20. Какой принцип лежит в основе управления доступом в облачных средах?

A) Все доступно всем

B) Принцип наименьших привилегий

C) Принцип максимальной доступности

D) Принцип единого доступа

Правильный ответ: B

21. Что такое Zero Trust Architecture?

A) Модель, которая предполагает доверие ко всем внутренним пользователям

B) Модель, которая не доверяет ни одному запросу по умолчанию

C) Модель, которая отключает все системы безопасности

D) Модель, которая доверяет только внешним пользователям

Правильный ответ: B

22. Какой метод шифрования подразумевает, что ключи шифрования хранятся у клиента, а не у провайдера?

A) BYOK (Bring Your Own Key)

B) SSE-S3 (Server-Side Encryption with S3-Managed Keys)

C) SSE-KMS (Server-Side Encryption with KMS)

D) SSE-C (Server-Side Encryption with Customer-Provided Keys)

Правильный ответ: A

23. Какой инструмент используется для обнаружения аномалий и угроз в облачных средах с использованием ИИ?

A) AWS GuardDuty

B) AWS EC2

C) AWS S3

D) AWS Lambda

Правильный ответ: A

24. Что такое CSPM (Cloud Security Posture Management)?

A) Управление облачными политиками безопасности

B) Мониторинг и оценка соответствия настроек облачной среды требованиям безопасности

C) Управление ключами шифрования

D) Управление доступом пользователей

Правильный ответ: B

Форма: Множественный выбор (25–27)
25. Какие компоненты входят в IAM-систему облачного провайдера? (Выберите все верные)

A) Пользователи

B) Группы

C) Роли

D) Политики доступа

Правильные ответы: A, B, C, D

26. Какие методы защиты данных в облаке используются для предотвращения утечек? (Выберите все верные)

A) Шифрование

B) DLP (Data Loss Prevention)

C) Управление ключами (KMS)

D) Дефрагментация дисков

Правильные ответы: A, B, C

27. Какие типы шифрования данных в облаке существуют? (Выберите все верные)

A) Шифрование на стороне клиента

B) Шифрование на стороне сервера

C) Шифрование в транзите

D) Шифрование в режиме реального времени

Правильные ответы: A, B, C

МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред
Форма: Одиночный выбор (28–29)
28. Какой механизм в Kubernetes используется для ограничения прав доступа пользователей и сервисных аккаунтов?

A) Pod Security Policies

B) RBAC (Role-Based Access Control)

C) Network Policies

D) Service Mesh

Правильный ответ: B

29. Какой инструмент используется для сканирования контейнерных образов на уязвимости?

A) Trivy

B) Kubectl

C) Docker Compose

D) Helm

Правильный ответ: A

Форма: Сопоставление (30)
30. Установите соответствие между инструментом безопасности облачных технологий и его функцией:

Инструмент Функция
1. Falco A. Сканирование контейнеров на уязвимости
2. OPA B. Политики безопасности для облачных и контейнерных сред
3. Trivy C. Мониторинг рантайма контейнеров
4. Kube-bench D. Аудит кластера Kubernetes на соответствие стандартам
Правильный ответ:

1 → C

2 → B

3 → A

4 → D

Примерные оценочные материалы
для проведения промежуточной аттестации (зачет, экзамен)
по итогам освоения дисциплины (модуля)

РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ВОПРОСЫ К ЗАЧЁТУ (30 вопросов)

Блок 1. Основы облачных технологий и архитектура безопасности (вопросы 1–10)

Дайте определение облачных вычислений. Перечислите и охарактеризуйте основные модели сервисов (IaaS, PaaS, SaaS, FaaS).

Какие модели развертывания облачных сред существуют? В чём их отличия?

Что такое модель разделения ответственности (Shared Responsibility Model) в облачных вычислениях? Приведите примеры.

Какие основные угрозы и риски характерны для облачных сред?

Что такое «мультиоблако» и какие дополнительные риски безопасности оно создаёт?

Какие нормативно-правовые акты РФ регулируют безопасность облачных вычислений?

Что такое виртуализация и как она влияет на безопасность облачных сред?

Какие требования предъявляются к физической безопасности облачных дата-центров?

В чём отличие безопасности публичного облака от частного облака?

Каковы основные принципы построения безопасной облачной архитектуры?

Блок 2. Управление доступом, защита данных и мониторинг (вопросы 11–20)

Что такое IAM (Identity and Access Management) в облачных средах? Опишите его основные компоненты.

Какие принципы управления доступом лежат в основе облачной безопасности (например, принцип наименьших привилегий)?

Что такое Zero Trust Architecture и как она применяется в облачных средах?

Какие методы шифрования данных используются в облачных средах? В чём разница между шифрованием на стороне клиента и на стороне сервера?

Что такое управление ключами шифрования (KMS)? Какие подходы к управлению ключами

существуют (BYOK, HYOK)?

Какие инструменты используются для мониторинга безопасности в облачных средах (на примере AWS/Azure/Yandex Cloud)?

Как применяются методы искусственного интеллекта и машинного обучения для мониторинга и обнаружения угроз в облаке?

Что такое Cloud Security Posture Management (CSPM) и для чего он используется?

Какие инструменты применяются для выявления аномалий и поведенческого анализа в облачных средах?

Что такое SIEM-системы и как они интегрируются с облачными платформами?

Блок 3. Безопасность контейнеров, оркестрации и управления уязвимостями (вопросы 21–30)
Какие основные угрозы связаны с использованием контейнеров (Docker)?

Что такое безопасность оркестрации Kubernetes? Перечислите ключевые механизмы защиты.

Что такое RBAC (Role-Based Access Control) в Kubernetes и как он настраивается?

Что такое Pod Security Policies, и как они применяются для усиления безопасности кластера?

Что такое Network Policies в Kubernetes и для чего они используются?

Какие инструменты применяются для сканирования контейнерных образов на уязвимости?

Что такое бессерверные вычисления (FaaS) и какие угрозы для них характерны?

Как обеспечить безопасность CI/CD-пайплайнов в облачных средах?

Что такое Infrastructure as Code (IaC) и как обеспечить безопасность инфраструктурного кода?

Какие практики и инструменты используются для управления уязвимостями в облачных средах?

РАЗДЕЛ 2. ЗАДАНИЯ НА ПРОВЕРКУ УМЕНИЙ (10 заданий)
Умение 1. Анализ модели разделения ответственности.

Задание 1.

Определите, какая сторона (провайдер или клиент) отвечает за следующие аспекты безопасности в модели IaaS: физическая безопасность дата-центра, защита гипервизора, настройка межсетевых экранов, обновление гостевой ОС, управление доступом к виртуальной машине. Ответ обоснуйте.

Умение 2. Проектирование политик IAM.

Задание 2.

Разработайте политику IAM для организации, использующей облачную платформу. Определите роли: администратор инфраструктуры, разработчик, оператор мониторинга, бухгалтер (только для биллинга). Для каждой роли укажите минимально необходимые разрешения.

Умение 3. Оценка рисков при переходе в облако.

Задание 3.

Компания планирует миграцию критического приложения в публичное облако. Выявите не менее 5 ключевых рисков безопасности, связанных с этим переходом. Предложите способы снижения каждого риска.

Умение 4. Выбор стратегии шифрования данных.

Задание 4.

Определите стратегию шифрования для следующих типов данных в облаке: базы данных, файлы в объектном хранилище, данные в транзите, резервные копии. Выберите методы шифрования и управления ключами для каждого типа.

Умение 5. Настройка мониторинга угроз с использованием ИИ.

Задание 5.

Спроектируйте систему мониторинга безопасности для облачной инфраструктуры с использованием ИИ-инструментов. Определите: какие источники данных собирать, какие типы аномалий выявлять, как организовать оповещение и автоматическое реагирование.

Умение 6. Разработка политики безопасности контейнеров.

Задание 6.

Разработайте политику безопасности для использования контейнеров Docker в организации. Включите правила по сканированию образов, ограничениям на запуск контейнеров, управлению секретами и мониторингу рантайма.

Умение 7. Проектирование Network Policies для Kubernetes.

Задание 7.

Для кластера Kubernetes с микросервисной архитектурой разработайте Network Policies, обеспечивающие сегментацию: веб-слой, бизнес-логика, база данных. Опишите правила для каждого компонента.

Умение 8. Безопасность бессерверных приложений.

Задание 8.

Разрабатывается бессерверное приложение на AWS Lambda/Yandex Cloud Functions, которое обращается к базе данных и объектному хранилищу. Составьте перечень мер безопасности: управление доступом, защита данных, мониторинг, защита от инъекций.

Умение 9. Безопасность CI/CD в облаке.

Задание 9.

Предложите комплекс мер по обеспечению безопасности CI/CD-пайплайна, развёрнутого в облачной среде. Включите защиту кода, артефактов, секретов, контроля доступа и аудита действий.

Умение 10. Разработка плана реагирования на инциденты в облаке.

Задание 10.

Разработайте план реагирования на инцидент безопасности в облачной среде для сценария: несанкционированный доступ к бакету с персональными данными. Опишите этапы, роли, действия, каналы коммуникации и взаимодействие с провайдером.

РАЗДЕЛ 3. ЗАДАНИЯ НА ПРОВЕРКУ НАВЫКОВ (10 заданий)

Навык 1. Создание IAM-пользователя и роли.

Задание 1.

В облачной консоли (фактически или на эмуляторе) создайте IAM-пользователя и привяжите к нему политику «только чтение» для одного сервиса (например, объектного хранилища). Предоставьте скриншоты и описание выполненных действий.

Навык 2. Настройка групп безопасности.

Задание 2.

Настройте группы безопасности (Security Groups) для виртуальной машины, разрешающие: SSH (порт 22) только с IP вашего администратора, HTTP (80) и HTTPS (443) из любой сети, доступ к БД (3306) только с IP сервера приложений. Опишите правила.

Навык 3. Настройка шифрования дисков.

Задание 3.

Настройте шифрование дисков для виртуальной машины и проверьте его состояние. Создайте ключ шифрования в KMS и примените его к существующему диску (или в процессе создания). Предоставьте скриншоты.

Навык 4. Настройка аудита и мониторинга.

Задание 4.

Настройте сбор логов действий пользователей (CloudTrail, Audit Logs) в облачной среде. Включите мониторинг неавторизованных попыток доступа и создайте алерт для указанного события.

Навык 5. Сканирование контейнерного образа на уязвимости.

Задание 5.

Сканируйте контейнерный образ (например, nginx) с использованием Trivy или аналогичного инструмента. Выявите найденные уязвимости, классифицируйте их по уровню критичности и предложите способы устранения.

Навык 6. Настройка RBAC в Kubernetes.

Задание 6.

Создайте Service Account в Kubernetes и привяжите к нему роль, позволяющую только читать Pod'ы в пространстве имён "development". Примените манифесты и проверьте работоспособность через kubectl.

Навык 7. Создание и применение Network Policy в Kubernetes.

Задание 7.

Разработайте и примените Network Policy в Kubernetes, запрещающую Pod'ам в пространстве имён "frontend" обращаться к Pod'ам в пространстве имён "database", за исключением одного разрешённого Pod'а. Проверьте результат.

Навык 8. Развертывание бессерверной функции с ограниченными правами.

Задание 8.

Разверните бессерверную функцию (AWS Lambda/Yandex Cloud Function), которая обращается к облачному объектному хранилищу. Настройте для функции роль с минимальными правами и проверьте работу.

Навык 9. Использование ИИ-инструмента для обнаружения аномалий.

Задание 9.

Настройте ИИ-инструмент мониторинга облачной безопасности (например, GuardDuty, Security Command Center). Проведите тестовую эмуляцию подозрительной активности и проанализируйте реакцию системы на аномалию.

Навык 10. Составление отчёта о соответствии (compliance).

Задание 10.

На основе настроенной облачной среды и политик безопасности составьте отчёт о соответствии требованиям по защите персональных данных (ФЗ-152 или GDPR). Включите оценку шифрования, управления доступом, аудита и контроля инцидентов.

Темы письменных работ (эссе, рефераты, курсовые работы и др.)

Темы рефератов:

МОДУЛЬ 1. Основы безопасности облачных инфраструктур

Модели облачных сервисов (IaaS, PaaS, SaaS, FaaS): сравнительный анализ и особенности обеспечения безопасности.

Цель: провести сравнение моделей сервисов с точки зрения распределения ответственности, угроз и методов защиты для каждой модели.

Модель разделения ответственности (Shared Responsibility Model) в облачных вычислениях: практические аспекты реализации.

Цель: детально разобрать модель разделения ответственности для различных облачных сервисов, показать на примерах, как она реализуется у основных провайдеров.

Сравнительный анализ моделей развертывания облачных сред: публичное, частное, гибридное, мультиоблако.

Цель: сравнить модели по критериям безопасности, стоимости, управляемости и соответствия нормативным требованиям.

Основные угрозы и уязвимости облачных сред: классификация, источники и методы противодействия.

Цель: систематизировать угрозы облачных сред (внешние, внутренние, технические, организационные) и предложить методы защиты.

Нормативно-правовое регулирование безопасности облачных вычислений в Российской Федерации.

Цель: проанализировать законодательство РФ (ФЗ-149, ФЗ-152, приказы ФСТЭК) применительно к использованию облачных сервисов.

Международные стандарты и требования к безопасности облачных технологий (ISO/IEC 27017, 27018, CSA STAR).

Цель: провести обзор международных стандартов, их структуры, требований и порядка сертификации облачных провайдеров.

Физическая безопасность облачных дата-центров: стандарты, практики, угрозы.

Цель: изучить требования к физической защите дата-центров, системы контроля доступа, противопожарной защиты, резервного электропитания.

МОДУЛЬ 2. Управление доступом, защита данных и ИИ-мониторинг

Управление идентификацией и доступом (IAM) в облачных средах: архитектура, компоненты, практики.

Цель: детально разобрать IAM-системы, включая пользователей, группы, роли, политики, сервисные аккаунты и федеративное управление доступом.

Zero Trust Architecture в облачных средах: принципы, реализация, вызовы.

Цель: рассмотреть концепцию Zero Trust, её применение в облаке, инструменты реализации и ограничения.

Технологии шифрования данных в облаке: методы, управление ключами, сценарии применения.

Цель: разобрать методы шифрования (на стороне клиента, сервера), подходы к управлению ключами (BYOK, HYOK), примеры реализации у провайдеров.

Data Loss Prevention (DLP) в облачных средах: методы, инструменты, ограничения.

Цель: рассмотреть подходы к предотвращению утечек данных в облаке, сравнительный анализ DLP-решений.

Применение искусственного интеллекта и машинного обучения для мониторинга безопасности облачных сред.

Цель: исследовать использование ИИ для обнаружения аномалий, прогнозирования угроз, поведенческого анализа в облаке на примерах конкретных инструментов.

Cloud Security Posture Management (CSPM) и Cloud Workload Protection Platforms (CWPP): сравнительный анализ.

Цель: сравнить подходы и инструменты для управления состоянием безопасности облачных сред и защиты рабочих нагрузок.

Интеграция SIEM-систем с облачными платформами: архитектура, сбор логов, анализ событий.

Цель: рассмотреть способы интеграции SIEM с облачными средами, сбор логов и метрик, корреляцию событий безопасности.

МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред

Безопасность контейнеров Docker: образы, реестры, рантайм-безопасность.

Цель: детально разобрать все аспекты безопасности контейнеров: создание защищённых образов, хранение в реестрах, ограничения в рантайме.

Безопасность оркестрации Kubernetes: архитектура, RBAC, Pod Security Policies, Network Policies.

Цель: рассмотреть механизмы безопасности Kubernetes, настройку контроля доступа, политик безопасности подов и сетевой сегментации.

Service Mesh и безопасность микросервисов в облачных средах (на примере Istio).

Цель: изучить применение Service Mesh для обеспечения безопасности микросервисов: mTLS, аутентификация, авторизация, мониторинг.

Безопасность бессерверных вычислений (FaaS): угрозы, методы защиты, мониторинг.

Цель: проанализировать специфические угрозы бессерверных архитектур и методы их нейтрализации (управление доступом, защита данных, инъекции).

Безопасность CI/CD-пайплайнов в облачных средах: защита кода, артефактов, секретов, IaC.

Цель: разобрать подходы к обеспечению безопасности пайплайнов поставки ПО в облаке, включая сканирование кода, защиту секретов и анализ Infrastructure as Code.

Инструменты безопасности контейнерных и облачных сред: Trivy, Falco, OPA, Kube-bench.

Цель: провести обзор и сравнительный анализ инструментов для сканирования уязвимостей, мониторинга рантайма и аудита конфигураций.