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.

Рабочая программа дисциплины

ФТД.01 Безопасность облачных технологий

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

очная

Ставрополь, 2026

1. Цель дисциплины

Цель освоения дисциплины — формирование у магистрантов системных компетенций в области обеспечения безопасности облачных вычислений, включая управление идентификацией и доступом, защиту данных, безопасность контейнерных и бессерверных сред, а также применение методов искусственного интеллекта для мониторинга и обнаружения угроз в облачной инфраструктуре.

2. 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 компетенции	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 ситуации на основе источников информации. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие	**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 **владеет навыками**

	дальнейшей разработке. Предлагает способы их решений	навыками поиска и систематизации информации, декомпозиции задач и выработки конкретных решений для облачной безопасности

3. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность облачных технологий» является дисциплиной факультативной части программы.

Изучение дисциплины осуществляется в 1семестре(-ах).

Для освоения дисциплины «Безопасность облачных технологий» студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин:

Освоение дисциплины «Безопасность облачных технологий» является необходимой основой для последующего изучения следующих дисциплин:

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

Технологическая (проектно-технологическая) практика

Преддипломная практика

Администрирование безопасных информационных систем

Администрирование защищенных сетей

Технологии непрерывной разработки и безопасности

Технологии расследования компьютерных преступлений и инцидентов

Технологии разработки защищенного ПО

Поведенческий анализ и мониторинг защищенности с использованием ИИ

Обнаружение и анализ вредоносного программного обеспечения

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Безопасность облачных технологий» в соответствии с рабочим учебным планом и ее распределение по видам работ представлены ниже.

Семестр	Трудоемкость час/з.е.	Контактная работа с преподавателем, час			Самостоятельная работа, час	Контроль, час	Форма промежуточной аттестации (форма контроля)
		лекции	практические занятия	лабораторные занятия			
1	72/2	8	16		48		За
в т.ч. часов: в интерактивной форме		2	4				

Семестр	Трудоемкость час/з.е.	Внеаудиторная контактная работа с преподавателем, час/чел					
		Курсовая работа	Курсовой проект	Зачет	Дифференцированный зачет	Консультации перед экзаменом	Экзамен
1	72/2			0.12			

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

№	Наименование раздела/темы	Семестр	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
			всего	Лекции	Семинарские занятия		Самостоятельная работа			
					Практические	Лабораторные				
1.	1 раздел. Безопасность облачных технологий									
1.1.	МОДУЛЬ 1. Основы безопасности облачных инфраструктур	1	4	2	2		15		Устный опрос	
1.2.	МОДУЛЬ 2. Управление доступом, защита данных и применение ИИ для мониторинга	1	8	2	6		18		Задачи	
1.3.	КТ 1	1	2		2			КТ 1	Тест	
1.4.	МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред	1	8	4	4		15		Задачи	
1.5.	КТ 2	1	2		2			КТ 2	Тест	
1.6.	Зачет	1							Тест	
	Промежуточная аттестация	За								
	Итого		72	8	16		48			
	Итого		72	8	16		48			

5.1. Лекционный курс с указанием видов интерактивной формы проведения занятий

Тема лекции (и/или наименование раздел) (вид интерактивной формы проведения занятий)/ (практическая подготовка)	Содержание темы (и/или раздела)	Всего, часов / часов интерактивных занятий/ практическая подготовка
МОДУЛЬ 1. Основы безопасности облачных инфраструктур	Архитектура облачных вычислений и основы безопасности	2/2
МОДУЛЬ 2. Управление доступом, защита данных и применение ИИ для мониторинга	Управление доступом, защита данных и ИИ-мониторинг в облачных средах	2/-
МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред	Безопасность контейнерных и бессерверных сред	4/-
Итого		8

5.2.1. Семинарские (практические) занятия с указанием видов проведения занятий в интерактивной форме

Наименование раздела дисциплины	Формы проведения и темы занятий (вид интерактивной формы проведения занятий)/(практическая подготовка)	Всего, часов / часов интерактивных занятий/ практическая подготовка	
		вид	часы
МОДУЛЬ 1. Основы безопасности облачных инфраструктур	Анализ модели разделения ответственности и настройка базовых политик безопасности	Пр	2/2/-
МОДУЛЬ 2. Управление доступом, защита данных и применение ИИ для мониторинга	Настройка IAM, шифрования и ИИ-мониторинга облачной инфраструктуры	Пр	6/2/-
КТ 1	Контрольная точка 1	Пр	2/-/-
МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред	Настройка безопасности контейнерной платформы и бессерверной среды	Пр	4/-/-
КТ 2	Контрольная точка 2	Пр	2/-/-
Итого			

5.3. Курсовой проект (работа) учебным планом не предусмотрен

5.4. Самостоятельная работа обучающегося

Темы и/или виды самостоятельной работы	Часы
Изучение пройденного материала и подготовка к практическому занятию	15
Изучение пройденного материала и подготовка к практическому занятию	18
Изучение пройденного материала и подготовка к практическому занятию	15

Зачет	0

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Учебно-методическое обеспечение для самостоятельной работы обучающегося по дисциплине «Безопасность облачных технологий» размещено в электронной информационно-образовательной сре-де Университета и доступно для обучающегося через его личный кабинет на сайте Университета. Учебно-методическое обеспечение включает:

1. Рабочую программу дисциплины «Безопасность облачных технологий».

2.Методические рекомендации для организации самостоятельной работы обучающегося по дисциплине «Безопасность облачных технологий».

3. Методические рекомендации по выполнению письменных работ () (при наличии).

4. Методические рекомендации по выполнению контрольной работы студентами заочной формы обучения (при наличии)

5. Методические указания по выполнению курсовой работы (проекта) (при наличии).

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)		
		основная (из п.8 РПД)	дополнительная (из п.8 РПД)	метод. лит. (из п.8 РПД)
1	МОДУЛЬ 1. Основы безопасности облачных инфраструктур. Изучение пройденного материала и подготовка к практическому занятию	Л1.1, Л1.3, Л1.4	Л2.1, Л2.2, Л2.3	Л3.2, Л3.3
2	МОДУЛЬ 2. Управление доступом, защита данных и применение ИИ для мониторинга. Изучение пройденного материала и подготовка к практическому занятию	Л1.1, Л1.3, Л1.4	Л2.1, Л2.2, Л2.3	Л3.2, Л3.3
3	МОДУЛЬ 3. Безопасность контейнеров, оркестрации и бессерверных сред. Изучение пройденного материала и подготовка к практическому занятию	Л1.1, Л1.3, Л1.4	Л2.1, Л2.2, Л2.3	Л3.2, Л3.3
4	Зачет. Зачет	Л1.1, Л1.3, Л1.4	Л2.1, Л2.2, Л2.3	Л3.2, Л3.3

7. Фонд оценочных средств (оценочных материалов) для проведения промежуточной аттестации обучающихся по дисциплине «Безопасность облачных технологий»

7.1. Перечень индикаторов компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индикатор компетенции (код и содержание)	Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетен-ции	

7.2. Критерии и шкалы оценивания уровня усвоения индикатора компетенций, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций по дисциплине «Безопасность облачных технологий» проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по её

корректировке, а также для совершенствования методики обучения, организации учебной работы и оказания индивидуальной помощи обучающемуся.

Промежуточная аттестация по дисциплине «Безопасность облачных технологий» проводится в виде Зачет.

За знания, умения и навыки, приобретенные студентами в период их обучения, выставляются оценки «ЗАЧТЕНО», «НЕ ЗАЧТЕНО». (или «ОТЛИЧНО», «ХОРОШО», «УДОВЛЕТВОРИТЕЛЬНО», «НЕУДОВЛЕТВОРИТЕЛЬНО» для дифференцированного зачета/экзамена)

Для оценивания знаний, умений, навыков и (или) опыта деятельности в университете применяется балльно-рейтинговая система оценки качества освоения образовательной программы. Оценка проводится при проведении текущего контроля успеваемости и промежуточных аттестаций обучающихся. Рейтинговая оценка знаний является интегрированным показателем качества теоретиче-ских и практических знаний и навыков студентов по дисциплине.

Состав балльно-рейтинговой оценки студентов очной формы обучения

Для студентов очной формы обучения знания по осваиваемым компетенциям формируются на лекционных и практических занятиях, а также в процессе самостоятельной подготовки.

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций	Максимальное количество баллов
1 семестр		
КТ 1	Тест	15
КТ 2	Тест	15
Сумма баллов по итогам текущего контроля		**30**
Посещение лекционных занятий		20
Посещение практических/лабораторных занятий		20
Результативность работы на практических/лабораторных занятиях		30
Итого		100

№ контрольной точки	Оценочное средство результатов индикаторов достижений компетенций	Максимальное количество баллов	Критерии оценки знаний студентов
1 семестр			
КТ 1	Тест	15	11-15 баллов выставляется обучающемуся, если тестовые задания выполняются на 85% и выше; 8-10 баллов выставляется обучающемуся, если тестовые задания выполняются на 70 - 84%; 5-7 баллов выставляется обучающемуся, если тестовые задания выполняются на 55 – 69 %; 1-4 балла выставляется обучающемуся, если тестовые задания выполняются на 45 – 54%; 0 баллов выставляется обучающемуся, если тестовые задания выполняются на 44% и меньше.

КТ 2	Тест	15	11-15 баллов выставляется обучающемуся, если тестовые задания выполняются на 85% и выше; 8-10 баллов выставляется обучающемуся, если тестовые задания выполняются на 70 - 84%; 5-7 баллов выставляется обучающемуся, если тестовые задания выполняются на 55 – 69 %; 1-4 балла выставляется обучающемуся, если тестовые задания выполняются на 45 – 54%; 0 баллов выставляется обучающемуся, если тестовые задания выполняются на 44% и меньше.

Критерии и шкалы оценивания результатов обучения на промежуточной аттестации

При проведении итоговой аттестации «зачет» («дифференцированный зачет», «экзамен») преподавателю с согласия студента разрешается выставлять оценки («отлично», «хорошо», «удовлетворительно», «зачет») по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет (дифференцированный зачет, экзамен) по приведенным выше вопросам и заданиям. Итоговая успеваемость (зачет, дифференцированный зачет, экзамен) не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче (зачета, дифференцированного зачета, экзамена) к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на (зачете, дифференцированном зачете, экзамене) и сумма баллов переводится в оценку.

Критерии и шкалы оценивания ответа на зачете

По дисциплине «Безопасность облачных технологий» к зачету допускаются студенты, выполнившие и сдавшие практические работы по дисциплине, имеющие ежемесячную аттестацию и без привязке к набранным баллам. Студентам, набравшим более 65 баллов, зачет выставляется по результатам текущей успеваемости, студенты, не набравшие 65 баллов, сдают зачет по вопросам, предусмотренным РПД. Максимальная сумма баллов по промежуточной аттестации (зачету) устанавливается в 15 баллов

Вопрос билета	Количество баллов
Теоретический вопрос	до 5
Задания на проверку умений	до 5
Задания на проверку навыков	до 5

Теоретический вопрос

5 баллов выставляется студенту, полностью освоившему материал дисциплины или курса в соответствии с учебной программой, включая вопросы рассматриваемые в рекомендованной программой дополнительной справочно-нормативной и научно-технической литературы, свободно владеющему основными понятиями дисциплины. Требуется полное понимание и четкость изложения ответов по экзаменационному заданию (билету) и дополнительным вопросам, заданных экзаменатором. Дополнительные вопросы, как правило, должны относиться к материалу дисциплины или курса, не отраженному в основном экзаменационном задании (билете) и выявляют полноту знаний студента по дисциплине.

4 балла заслуживает студент, ответивший полностью и без ошибок на вопросы экзаменационного задания и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.

3 балла дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и

несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.

2 балла дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

1 балл дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

0 баллов - при полном отсутствии ответа, имеющего отношение к вопросу.

Задания на проверку умений и навыков

5 баллов Задания выполнены в обозначенный преподавателем срок, письменный отчет без замечаний. Работа выполнена в полном объеме с соблюдением необходимой последовательности.

4 балла Задания выполнены в обозначенный преподавателем срок, письменный отчет с небольшими недочетами.

2 баллов Задания выполнены с задержкой, письменный отчет с недочетами. Работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы.

1 баллов Задания выполнены частично, с большим количеством вычислительных ошибок, объем выполненной части работы не позволяет сделать правильных выводов.

0 баллов Задания выполнены, письменный отчет не представлен или работа выполнена не полностью, и объем выполненной части работы не позволяет сделать правильных выводов.

7.3. Примерные оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Безопасность облачных технологий»

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 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.
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

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

основная

Л1.1 Дергачев К. В., Титарев Д. В. Защита информации: лабораторный практикум [Электронный ресурс]:учеб. пособие ; ВО - Бакалавриат, Магистратура. - Москва: Русайнс, 2024. - 158 с. – Режим доступа: https://book.ru/book/952795

Л1.2 Баланов А. Н. Защита информационных систем. Кибербезопасность [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат. - Санкт-Петербург: Лань, 2024. - 280 с. – Режим доступа: https://e.lanbook.com/book/394544

Л1.3 Емелина Е. И. Поддержка и тестирование программных модулей [Электронный ресурс]:учебник для СПО. - Москва: КноРус, 2024. - 267 с. – Режим доступа: https://book.ru/book/954267

Л1.4 Игнатьев А. В. Тестирование программного обеспечения [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат. - Санкт-Петербург: Лань, 2025. - 56 с. – Режим доступа: https://e.lanbook.com/book/481331

дополнительная

Л2.1 Ищейнов В. Я. Информационная безопасность и защита информации [Электронный ресурс]:словарь терминов и понятий. - Москва: Русайнс, 2026. - 226 с. – Режим доступа: https://book.ru/book/959878

Л2.2 Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И. Защита информации [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат, Магистратура, Специалитет, Аспирантура. - Москва: Издательский Центр РИО□, 2026. - 398 с. – Режим доступа: https://znanium.ru/catalog/document?id=480737

Л2.3 Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат. - Москва: Издательский Центр РИО□, 2026. - 384 с. – Режим доступа: https://znanium.ru/catalog/document?id=477891

б) Методические материалы, разработанные преподавателями кафедры по дисциплине, в соответствии с профилем ОП.

Л3.1 Клименко И. С. Информационная безопасность и защита информации: модели и методы управления [Электронный ресурс]:моногр.. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2024. - 180 с. – Режим доступа: https://znanium.com/catalog/document?id=431346

Л3.2 Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат. - Москва: Издательский Центр РИО□, 2024. - 336 с. – Режим доступа: https://znanium.ru/catalog/document?id=442107

Л3.3 Баланов А. Н. Защита информационных систем. Кибербезопасность [Электронный ресурс]:учеб. пособие для СПО. - Санкт-Петербург: Лань, 2026. - 84 с. – Режим доступа: https://e.lanbook.com/book/515089

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

№	Наименование ресурса сети «Интернет»	Электронный адрес ресурса
1	Классический учебник по сетевой безопасности	https://cat.gpntb.ru/index.php?id=EC/ShowFull&irbDb=ESVODT&bid=a19b19000959c1567fbdbbc8dbdb9ae0
2	Современная монография по ML для кибербезопасности	https://ebooks.mpdl.mpg.de/ebooks/Record/EB002249738

10. Методические указания для обучающихся по освоению дисциплины

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ
ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель: сформировать у магистрантов системные компетенции в области обеспечения безопасности облачных вычислений, включая управление идентификацией и доступом, защиту данных, безопасность контейнерных и бессерверных сред, а также применение методов искусственного интеллекта для мониторинга и обнаружения угроз в облачной инфраструктуре.

Задачи освоения дисциплины:

изучить модели облачных сервисов (IaaS, PaaS, SaaS, FaaS) и модели развертывания;

освоить методы управления идентификацией и доступом (IAM), включая Zero Trust Architecture;

изучить технологии защиты данных в облаке: шифрование, управление ключами, DLP, защита API;

освоить инструменты мониторинга безопасности с применением ИИ и машинного обучения;

сформировать навыки обеспечения безопасности контейнерных (Docker, Kubernetes) и бессерверных сред;

изучить вопросы соответствия нормативным требованиям (ФЗ-152, GDPR, PCI DSS).

2. МЕСТО ДИСЦИПЛИНЫ В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к профессиональному циклу магистратуры по профилю «Искусственный интеллект в кибербезопасности».

Для успешного освоения требуются знания:

основ информационной безопасности и сетевых технологий;

принципов построения распределенных систем;

основ виртуализации и администрирования ОС;

базовых навыков работы с командной строкой и скриптовыми языками.

3. ОБЪЁМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ НАГРУЗКИ

Вид работы Объём (ориентировочно)
Лекции 10–14 часов
Практические занятия 10–14 часов
Самостоятельная работа 30–40 часов
Промежуточная аттестация (зачёт) 5–10 часов
Общая трудоёмкость 2–3 ЗЕТ (72–108 часов)

4. СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛИ)

Модуль Название Основное содержание
Модуль 1 Основы безопасности облачных инфраструктур Архитектура облачных вычислений, модели сервисов (IaaS, PaaS, SaaS, FaaS), модели развертывания, Shared Responsibility Model, угрозы, нормативное регулирование
Модуль 2 Управление доступом, защита данных и ИИ-мониторинг IAM, Zero Trust, шифрование и управление ключами, DLP, применение ИИ для мониторинга, CSPM, SIEM
Модуль 3 Безопасность контейнеров, оркестрации и бессерверных сред
Безопасность Docker, Kubernetes (RBAC, Pod Security, Network Policies), бессерверные вычисления (FaaS), безопасность CI/CD, инструменты (Trivy, Falco, OPA)

5. РЕКОМЕНДАЦИИ ПО РАБОТЕ С РАЗЛИЧНЫМИ ФОРМАМИ ЗАНЯТИЙ

5.1. Подготовка к лекциям

Перед лекцией: ознакомьтесь с предыдущим материалом, сформулируйте вопросы по неясным моментам.

Во время лекции: фиксируйте ключевые определения, модели, названия сервисов и инструментов.

После лекции: в течение 24 часов повторите материал, дополните конспект из официальной документации облачных провайдеров.

5.2. Подготовка к практическим занятиям

Повторите лекционный материал по соответствующей теме.

Изучите документацию используемого облачного провайдера (Yandex Cloud, VK Cloud, AWS, Azure).

Заранее создайте тестовый аккаунт с ограниченными правами (Free Tier или учебный грант).

В процессе работы фиксируйте выполненные команды, настройки, ошибки и способы их устранения.

Оформляйте отчёт по каждому практическому занятию с описанием этапов и скриншотами.

5.3. Самостоятельная работа

Изучайте официальную документацию облачных провайдеров (она наиболее актуальна и достоверна).

Ведите глоссарий терминов (IAM, KMS, CSPM, SIEM, Zero Trust, RBAC, VPC, ACL, TLS и др.).

Отрабатывайте навыки на бесплатных облачных ресурсах.

Сравнивайте подходы различных провайдеров к безопасности.

6. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ОТЧЁТОВ ПО ПРАКТИЧЕСКИМ РАБОТАМ

Каждый отчёт должен содержать:

Раздел Содержание
Цель работы Формулировка задачи

Используемые сервисы и инструменты Перечень с кратким обоснованием выбора
Ход выполнения Пошаговое описание действий с командами и скриншотами
Результаты Что удалось настроить/проверить
Выводы Анализ полученных результатов, оценка эффективности настроек

7. РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАЧЁТУ

Систематизируйте материал по трём модулям дисциплины.

Проработайте теоретические вопросы (30 вопросов) — акцентируйте внимание на моделях сервисов, угрозах, нормативных требованиях и методах защиты.

Повторите задания на умения (10 заданий) — анализ, проектирование, обоснование решений.

Выполните тренировочное тестирование (30 заданий разных форм) для самопроверки.

Подготовьте краткие конспекты-схемы по каждому модулю.

Отработайте аргументацию выбора конкретных облачных сервисов и методов защиты для различных сценариев.

8. РЕКОМЕНДУЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ

Ресурс Назначение
Yandex Cloud / VK Cloud / AWS / Azure Официальная документация и руководства
Cloud Security Alliance (CSA) Стандарты и лучшие практики облачной безопасности
NIST SP 800-144, 800-145 Руководства по облачным вычислениям и безопасности
ФЗ-152 «О персональных данных» Законодательные требования
OWASP Cloud Security Практики безопасности облачных приложений
Docker / Kubernetes документация Безопасность контейнеров и оркестрации

9. ОБЩИЕ СОВЕТЫ ПО УСПЕШНОМУ ОСВОЕНИЮ ДИСЦИПЛИНЫ

Совет Пояснение
Изучайте документацию провайдеров Это первичный источник информации — он наиболее актуален
Практикуйтесь на бесплатных ресурсах Без практики теоретические знания теряют ценность
Сравнивайте провайдеров Понимание различий (AWS vs Azure vs Yandex) расширяет профессиональный кругозор
Применяйте принцип наименьших привилегий Это золотое правило безопасности в облаке
Автоматизируйте проверки Используйте Infrastructure as Code и сканирование конфигураций
Следите за новостями Облачные технологии и угрозы быстро меняются
Консультируйтесь с преподавателем При возникновении сложностей обращайтесь на занятиях или в консультационные часы

10. КОНТРОЛЬ И ОБРАТНАЯ СВЯЗЬ

Форма контроля Периодичность Что проверяется
Устный опрос на занятиях Каждое занятие Теоретические знания
Отчёт по практической работе После каждого занятия Навыки настройки облачных сервисов
Реферат 1 раз в семестр Умение анализировать литературу
Тренировочное тестирование По завершении модулей Знание терминологии, сервисов и методов защиты
Зачёт Конец семестра Все компетенции (знания, умения, навыки)

11. ЗАКЛЮЧИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ

Безопасность облака — это общая ответственность. Всегда понимайте, за что отвечаете вы, а за что — провайдер.

Учитесь на практике. Используйте бесплатные облачные ресурсы для отработки навыков.

Применяйте системный подход. Рассматривайте безопасность облачной инфраструктуры как единую систему, а не набор отдельных настроек.

Используйте ИИ-инструменты мониторинга. Они помогают обнаруживать угрозы, которые трудно заметить вручную.

Документируйте свои решения. Это пригодится не только на зачёте, но и в профессиональной деятельности.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства и информационных справочных систем (при необходимости).

11.1 Перечень лицензионного программного обеспечения

1. Kaspersky Endpoint Security 12.11 - Антивирус
2. Microsoft Windows Server STDCORE AllLngLicense/Software AssurancePack Academic OLV 16Licenses LevelE AdditionalProduct CoreLic 1Year - Серверная операционная система

11.3 Перечень программного обеспечения отечественного производства

1. Kaspersky Endpoint Security 12.11 - Антивирус

При осуществлении образовательного процесса студентами и преподавателем используются следующие информационно справочные системы: СПС «Консультант плюс», СПС «Гарант».

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Номер аудитории	Оснащенность специальных помещений и помещений для самостоятельной работы

1	Учебная аудитория для проведения занятий всех типов (в т.ч. лекционного, семинарского, практической подготовки обучающихся), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	315/НК	Оснащение: специализированная мебель на 250 посадочных мест, трибуна для лектора – 1 шт., президиум – 1 шт., видеостена из 9 бесшовный ЖК дисплеев Mercury Full HD 55” ширина-3,1 м высота - 1,7 м , АРМ на основе Intel Core i3 , Монитор Dell 21.5", Клавиатура + мышь , Источник бесперебойного питания 650ВА, Монитор ЖК размер экрана: Dell 21.5", широкоформатная матрица VA с разрешением 1920×1080, отношением сторон 16:9 - 3шт.,микрофонная система Restmoment RX-812 -1шт, Restmoment RX-D58 микрофон делегата -4шт.,АМС настенный громкоговоритель мониторного типа - 6шт., DSPPA микшер-усилитель - 1шт., магнитно-маркерная доска – 1 шт., учебно-наглядные пособия в виде тематических презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
		423/НК	Оснащение: специализированная мебель на 56 посадочных мест, стол преподавателя – 1 шт., Sharp 70" Информационный ЖК-дисплей – 1 шт., магнитно-маркерная доска – 1 шт., учебно-наглядные пособия в виде тематических презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
2	Помещение для самостоятельной работы обучающихся, подтверждающее наличие материально-технического обеспечения, с перечнем основного оборудования		

13. Особенности реализации дисциплины лиц с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточная аттестация может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточная аттестация проводится в устной форме.

Рабочая программа дисциплины «Безопасность облачных технологий» составлена на основе Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916).

Автор (ы)

_____ доцент КИТ, кэн Березницкий Андрей Сергеевич

Рецензенты

_____ доцент КИС, ктн Трошков Александр Михайлович

_____ доцент КИС, ктн Горяинов Михаил Федорович

Рабочая программа дисциплины «Безопасность облачных технологий» рассмотрена на заседании Кафедра информационных систем протокол № 9 от 06.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Заведующий кафедрой _____ Шлаев Дмитрий Валерьевич

Рабочая программа дисциплины «Безопасность облачных технологий» рассмотрена на заседании учебно-методической комиссии Факультет цифровых технологий протокол № 2 от 08.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Руководитель ОП _____