МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность распределенных компьютерных систем»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ Е.С. Соколова

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ К.А. Разинкин

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является формирование целостного представления об организации информационной безопасности распределённых компьютерных систем, получение теоретических знаний о принципах построения и архитектуре подобных систем.

1.2. Задачи освоения дисциплины

- сформировать у студентов представление о теоретических основах функционирования отказоустойчивых распределенных систем, связанных с защитой ресурсов (в частности, информации), заключающихся в создании механизма, исключающего несанкционированный доступ к ресурсам; защиты систем связи, состоящей в разработке мер противодействия угрозам активного и пассивного перехвата информации, передаваемой по сетям связи; аутентификации пользователей.
- предоставить студентам возможности освоения практических вопросов реализации распределенных алгоритмов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность распределенных компьютерных систем» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПОДИСЦИПЛИНЕ

Процесс изучения дисциплины «Безопасность распределенных компьютерных систем» направлен на формирование следующих компетенций:

ПК-4.5 - Способен анализировать уязвимости и угрозы информационной безопасности в компьютерных системах и сетях

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4.5	знать теоретические основы защиты функционирования отказоустойчивых распределенных систем
	уметь анализировать уязвимости и угрозы информационной безопасности в распределённых компьютерных системах и сетях
	владеть методами оценки риска, связанного с осуществлением угроз безопасности в отношении распределённой компьютерной системы

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Безопасность распределенных компьютерных систем» составляет 8 з.е. Распределение трудоемкости дисциплины по видам занятий.

очная форма обучения

Виды учебной работы	Всего часов	Семестр	
		9	А
Аудиторные занятия (всего)	108	54	54
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	36	18	18
Лаб.пр.подготовка	12	6	6
Самостоятельная работа	144	18	126
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет, зачет с оценкой	+	+	+
Общая трудоемкость: академические часы зач.ед.	288 8	72 2	216 6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий <u>очная форма обучения</u>

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Лаб.пр. подготовка	Всего, час
1	Введение в распределённые системы	**Вводная часть.** Понятие распределенной системы. Особенности распределенных систем. Примеры и применения. Параллельные и распределенные системы. Архитектурные особенности: сервисы, роли и архитектурные стили; клиент-сервер; одноранговые сети; сервисно-ориентированная архитектура. Дизайн масштабируемых распределенных систем: масштабируемость; особенности проектирования распределенных систем. **Модели.** Введение в моделирование и понятие модели. Модель распределенного	36	18	18	6	78

		исполнения: общее описание; модель коммуникационного канала; событийное описание; упорядочивание событий. Отношение причинного предшествования. Логическое время. Отметки времени Лампорта: реализация логических часов; скалярное время; векторное время; алгоритмы реализации векторных часов. Синхронное и асинхронное исполнение: введение; эмуляции синхронных систем асинхронными и наоборот. Модели отказов: отказы процессов; отказы коммуникационных каналов; иерархия моделей неисправности. Свойства распределенных алгоритмов. Глобальное состояние: распределенная сборка мусора; распределенное обнаружение тупиков; распределенное обнаружение завершения; фиксация глобального состояния. **Коммуникационная подсистема.** Введение и состав коммуникационной подсистемы. Состав коммуникационной подсистемы. Сети и сетевые технологии: типы сетей; ключевые проблемы использования сетей в распределенных системах; принципы построения сетей. Маршрутизация и алгоритмы на графах: графы; алгоритмы маршрутизации. Межпроцессный обмен: особенности обмена сообщениями; адресация, широковещательные и многоадресные рассылки, IP-multicast. Удаленные вызовы: протокол «запрос-ответ» (request-reply); удаленный вызов процедуры; пример удаленного вызова — веб					

		сервисы. Косвенные (indirect) коммуникации: очереди сообщений. Групповые коммуникации: координация и согласие в групповых коммуникациях, базовые многоадресные рассылки, надежная многоадресная рассылка, упорядоченные многоадресные рассылки, открытые группы и виртуальная синхронность **Синхронизация** Введение. Алгоритмы синхронизации часов: алгоритм Кристиана; алгоритм Беркли; усредняющие алгоритмы. Алгоритмы выбора. Распределенное взаимоисключение. Консенсус: введение; модель системы и основные определения; согласие в системах с отказами; отсутствие детерминированного решения в асинхронных системах; способы обхода результата FLP impossibility; алгоритм PAXOS. Распределенные транзакции: введение; свойства ACID; типы транзакций; компоненты архитектуры, необходимые для поддержки распределенных транзакций; управление параллельным выполнением транзакций; метод временных меток; контроль параллельного исполнения транзакций в некоторых популярных распределенных системах; протоколы распределенного завершения; восстановление после отказов; создание контрольных точек и откат путем восстановления **Репликация и консистентность** Введение. Модель и архитектура управления реплицированными данными. Пассивная и активная репликации.					

		Отказоустойчивость сервиса репликации. Модели консистентности: модели непротиворечивости, ориентированные на данные; модели непротиворечивости, ориентированные на клиента. Потенциальная согласованность; протоколы кворума. Размещение и обновление реплик **Системы хранения данных** Введение. Краткий обзор современных подходов к построению систем распределенного хранения данных: программно-определяемые хранилища; механизм хранения данных на уровне объектов; архитектурные особенности; механизм регулируемой избыточности; механизм георепликации; Проблемы теоремы CAP. Распределенные кластерные файловые системы. Пиринговые системы: одноранговые (пиринговые) сети; масштабируемость P2P-сетей; BitTorrent; DHT — распределенные хеш-таблицы; безопасность P2P-сетей; некоторые меры защиты P2P сетей					
2	Проектирование РИС	Технологии и платформы распределённой обработки больших данных Apache Hadoop: HDFS, MapReduce. Apache Spark: архитектура распределённого приложения, основные концепции (RDD, основные этапы обработки данных, загрузка данных из внешнего хранилища, управление памятью); Data Frame API и Spark SQL; создание, настройка и запуск Spark проекта Знакомство с контейнерными технологиями и платформами Docker и Kubernetes	18	9	63	3	93

		Облачные вычисления: модели развёртывания: частное и публичное, общественное и гибридное облака. Модели обслуживания: программное обеспечение как услуга; платформа как услуга; инфраструктура как услуга. Архитектурные шаблоны (паттерны) проектирования РС. Одноузловые паттерны проектирования Паттерн Sidecar Пример реализации паттерна Sidecar. Добавление возможности HTTPS-соединения к унаследованному сервису Динамическая конфигурация с помощью паттерна Sidecar Модульные контейнеры приложений Паттерн Ambassador Использование паттерна Ambassador для шардирования сервиса Использование паттерна Ambassador для реализации сервиса-посредника Использование паттерна Ambassador для проведения экспериментов и разделения запросов Паттерны проектирования обслуживающих систем Введение в микросервисы. Реплицированные сервисы с распределением нагрузки. Сервисы без внутреннего состояния. Датчики готовности для балансировщика нагрузки. Сервисы с закреплением сессий. Сервисы с репликацией на уровне приложения. Шардированные сервисы. Шардирование кэша. Шардирующие функции. Шардирование реплицированных сервисов. Системы с «горячим» шардированием. Функции и событийно-ориентированная обработка. Паттерны FaaS.					

		Событийно-ориентированная пакетная обработка. Паттерны событийно-ориентированной обработки: Паттерн Copier. Паттерн Filter. Паттерн Splitter. Паттерн Sharder. Паттерн Merger					
3	Безопасность РИС	**Безопасность систем BigData.** Особенности реализации информационной безопасности (далее ИБ) в озере данных Hadoop. Специфические угрозы ИБ существующие в озере данных. Организационные меры по ИБ для озера данных. Обзор подсистем безопасности озера данных: автоматизация; аутентификация и защита периметра; авторизация; аудит. Защита данных: шифрование данных; антивирусная защита данных; snapshots; репликация данных; резервное копирование и восстановление данных. Безопасные протоколы Kerberos и шифрование SSL. Настройки интегрированной безопасности компонент экосистемы Hadoop для унифицированного входа с использованием Single-Sign-On. Использование шлюза безопасности Apache Knox Gateway. Политики разграничения доступа Apache Ranger. Защита данных **HDFS**: шифрование данных при передаче; SSL шифрование для подключения к WebUI компонент экосистемы Hadoop; управление доступом к HDFS; антивирусная защита в озере данных **Безопасность контейнерными технологий и платформ (Docker и Kubernetes)** Защита сервера API Kubernetes: аутентификация, RBAC – защита кластера. Защита узлов и кластера и сети: использование в модуле	18	9	63	3	93

		пространств имён хоста, конфигурирование контекста безопасности контейнера, изоляция сети модуля. Обеспечение безопасности контейнеров на базе Docker: принцип минимальных привилегий; обеспечение безопасности identidock; подтверждение происхождения образов; механизм подтверждения контента в Docker; обеспечение безопасной загрузки ПО в файлах Dockerfile; рекомендации по обеспечению безопасности. Безопасность облачных вычислений. Границы безопасности. Модель стека Cloud Security Alliance (CSA). Контроль доступа. Аудиторская проверка. Аутентификация. Авторизация. Изолированный доступ к данным:Brokered Cloud Storage Access. Работа брокерской облачной системы доступа к хранилищу.					
Итого			72	36	144	12	264

5.2 Перечень лабораторных работ

1. Административные возможности управления системой безопасности DCOM.
2. Обеспечение безопасности при использовании компонентов ActiveX.
3. Проектирование распределенной базы данных
4. Манипуляция данными в системах распределенных баз данных.
5. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия.
6. Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server.
7. Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA.
8. Исследование и развертывание сетевой инфраструктуры Microsoft Windows Exchange Server

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта: «Исследование защищённости распределённой информационной системы предприятия»

Задачи, решаемые при выполнении курсового проекта:

- Анализ информационных ресурсов предприятия
- Формирование политики безопасности предприятия с учетом горизонтального масштабирования информационно-телекоммуникационной инфраструктуры
- разработка предложений по повышению эффективности обеспечения целостности, конфиденциально и доступности информационного обмена с учетом распределённого характера инфокоммуникационных ресурсов предприятия.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе: «аттестован»;«не аттестован».

Компетенция	Результаты обучения, характеризующие	Критерии оценивания	Аттестован	Не аттестован
ПК-4.5	знать теоретические основы защиты функционирования отказоустойчивых распределенных систем	Даёт определение понятиям «отказоустойчивость», «репликация», «консенсус», «распределенная транзакция». Перечисляет основные модели отказов (fail-stop, byzantine, crash, omission).Описывает принципы синхронизации времени и состояния в распределенных системах.Воспроизводит один из протоколов обеспечения отказоустойчивости (Paxos, Raft, 2PC/3PC) .Характеризует угрозы, специфичные для распределенных систем (атаки на синхронизацию, расщепление сознания (split-brain), нарушение целостности реплик).	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать уязвимости и угрозы информационной безопасности в распределённых компьютерных системах и сетях	Выявляет уязвимости в протоколах синхронизации и репликации данных.Классифицирует угрозы для распределенной системы по источнику (внешние/внутренние) и по воздействию (доступность, целостность, конфиденциальность).Интерпретирует результаты мониторинга распределенной системы с точки зрения безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами оценки риска, связанного с осуществлением угроз безопасности в отношении распределённой компьютерной системы	Применяет методики оценки риска (например, на основе ГОСТ/ISO 27005) к распределенной системе.Ранжирует риски по вероятности реализации и величине потенциального ущерба.Разрабатывает сценарии реализации угроз (по аналогии с MITRE ATT&CK для распределенных систем).	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, А семестре для очной формы обучения по четырехбалльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-4.5	знать теоретические основы защиты функционирования отказо-	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 7080%	В тесте менее 70% правильных ответов
	уметь анализировать уязвимости и угрозы информационной безопасности в распределённых компьютерных системах и сетях	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть методами оценки риска, связанного с осуществлением угроз безопасности в отношении распределённой ком-	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Какая модель отказа предполагает, что узел может вести себя произвольно (злонамеренно) и рассылать противоречивую информацию разным узлам?

А) Crash (отказ-остановка)

Б) Fail-stop (отказ с остановкой)

В) Omission (отказ-умолчание)

Г) Byzantine (византийский отказ)

2. Какой протокол консенсуса разработан специально для обеспечения отказоустойчивости в распределенных системах и использует понятие "лидера" (leader) и "терма" (term)?

А) Two-Phase Commit (2PC)

Б) Raft

В) Gossip Protocol

Г) Chord DHT

3. Что означает понятие "Split-Brain" (расщепление сознания) в распределенной системе?

А) Потерю данных при передаче по сети

Б) Разделение кластера на изолированные части, каждая из которых считает себя главной

В) Одновременный выход из строя всех узлов

Г) Несовместимость версий протоколов

4. Какая атака направлена на нарушение синхронизации времени в распределенной системе, что может привести к некорректной работе протоколов консенсуса?

А) ARP-spoofing

Б) NTP-amplification (атака на протокол точного времени)

В) SQL-инъекция

Г) XSS-атака

5. В распределенной системе хранения данных с репликацией злоумышленник перехватил и модифицировал данные при передаче от клиента к узлу хранения. Какое свойство безопасности нарушено в первую очередь?

А) Доступность

Б) Конфиденциальность

В) Целостность

Г) Аутентичность

6. Какая угроза характерна именно для распределенных систем, использующих механизм "quorum" (кворум) для принятия решений?

А) DDoS-атака на один узел

Б) Невозможность собрать кворум из-за сетевого разделения (network partition)

В) Переполнение буфера на сервере

Г) Подбор пароля администратора

7. В архитектуре распределенной системы присутствует единый координатор (оркестратор), который управляет всеми узлами. Какая уязвимость присуща такой архитектуре?

А) Отсутствие шифрования

Б) Single Point of Failure (единая точка отказа)

В) Низкая скорость обработки запросов

Г) Сложность масштабирования

8. При анализе системы на основе микросервисов обнаружено, что все сервисы используют один общий токен аутентификации. К какой уязвимости это приводит?

А) Компрометация одного сервиса приведет к компрометации всех

Б) Увеличивается скорость работы
В) Упрощается мониторинг
Г) Повышается отказоустойчивость

9. При оценке риска для распределенной базы данных выявлена угроза: "потеря целостности данных при отказе канала связи между центрами обработки данных (ЦОД)". Какой метод снижения риска наиболее эффективен?
А) Установка антивируса
Б) Асинхронная репликация с возможностью разрешения конфликтов
В) Отказ от репликации
Г) Увеличение частоты смены паролей

10. Что из перечисленного относится к идентификации риска (первый этап оценки риска)?
А) Расчет годовых потерь (ALE)
Б) Определение перечня угроз, актуальных для системы
В) Внедрение системы резервного копирования
Г) Тестирование на проникновение

11. Какой протокол используется для обеспечения безопасности и синхронизации в кластерных решениях (например, в Kubernetes и etcd) и основан на алгоритме консенсуса?
А) OAuth 2.0
Б) Raft
В) SAML
Г) LDAP

12. Для защиты распределенной системы от атак типа "Man-in-the-Middle" (перехват и модификация сообщений между узлами) необходимо использовать
А) Антивирусы на каждом узле
Б) Шифрование каналов связи и взаимную аутентификацию узлов (mTLS)
В) Балансировку нагрузки
Г) Регулярное резервное копирование

7.2.2 Примерный перечень заданий для решения стандартных задач

1. В распределенной системе хранения данных произошел сбой. Логи показывают, что узел А перестал отвечать на запросы, но другие узлы считают его "живым" и пытаются установить соединение. Какая модель отказа наиболее вероятна?
А) Crash (полная остановка)
Б) Fail-stop (остановка с уведомлением)
В) Omission (пропуск сообщений)
Г) Byzantine (византийская)

2.Компания разрабатывает распределенную систему для банковских транзакций. Критически важна целостность данных, даже если это замедлит работу. Какой механизм репликации следует выбрать?

А) Асинхронная репликация

Б) Синхронная репликация с подтверждением от всех реплик

В) Кэширование данных на клиентах

Г) Отказ от репликации

3.В логах распределенной системы обнаружены записи

Узел-координатор: Получен запрос на транзакцию TX-101

Узел-координатор: Отправлен prepare (подготовка) узлам A, B, C

Узел-координатор: Получен YES от A, B, C

Узел-координатор: Отправлен commit

Узел A: commit выполнен

Узел B: commit выполнен

-- Связь с узлом C потеряна --

В каком состоянии находится транзакция?

А) Полностью отменена

Б) Частично выполнена (узел C не зафиксировал данные)

В) Выполнена полностью на всех узлах

Г) Ожидает повторной попытки

4.В архитектуре микросервисов все внутренние запросы между сервисами передаются по HTTP без шифрования. Каждый сервис аутентифицирует входящие запросы по IP-адресу отправителя. Какая уязвимость присутствует?

А) Отсутствие резервного копирования

Б) Подмена IP-адреса (IP-spoofing) и перехват трафика

В) Медленная работа сервисов

Г) Сложность масштабирования

5.Схема распределенной системы:

Балансировщик нагрузки (1 экземпляр)

3 веб-сервера

1 сервер базы данных (master)

2 реплики БД (slave для чтения)

Что является единой точкой отказа (Single Point of Failure)?

А) Веб-серверы

Б) Балансировщик нагрузки

В) Реплики БД

Г) Сеть передачи данных

6. Администратор обнаружил, что кластер из 7 узлов разделился на две изолированные группы: 4 узла и 3 узла. Обе группы считают себя основными и принимают запись данных. Что необходимо сделать в первую очередь?

А) Продолжить работу в обеих группах

Б) Принудительно остановить группу из 3 узлов и восстановить данные из резервной копии

В) Объединить группы без остановки

Г) Перезагрузить все узлы одновременно

7.В распределенной файловой системе обнаружены три проблемы:

1. Отсутствует мониторинг загрузки дисков

2. Уязвимость в протоколе синхронизации позволяет злоумышленнику вызвать отказ узла

3. Не настроено резервное копирование метаданных

Какую проблему нужно устранить в первую очередь?

А) Отсутствие мониторинга

Б) Уязвимость в протоколе синхронизации

В) Отсутствие резервного копирования метаданных

Г) Все одновременно

8. В распределенной системе, размещенной в трех географически распределенных ЦОДах, оценивается риск "отказ всех ЦОДов одновременно из-за природной катастрофы". Какова примерная вероятность данного события?

А) Высокая (ежедневно)

Б) Средняя (раз в месяц)

В) Низкая (географическое распределение снижает вероятность)

Г) Нулевая

9.Для распределенной системы критичность риска (уровень риска) определяется по формуле: Риск = Вероятность × Ущерб.

Угроза "DDoS на координатор кластера" имеет:

Вероятность: Высокая (3 балла)

Ущерб: Критический (3 балла). Какой уровень риска (по 5-балльной шкале)?

А) Низкий (1-2)

Б) Средний (3-4)

В) Высокий (5-6)

Г) Критический (9)

10. Система критической инфраструктуры должна функционировать даже при наличии злонамеренных (скомпрометированных) узлов, которые могут рассылать ложную информацию. Какой подход необходим?

А) Использовать один супервизор

Б) Внедрить алгоритмы византийской отказоустойчивости (PBFT)

В) Отключить все узлы для проверки

Г) Использовать асинхронную репликацию

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Что понимается под термином наложение рутины на вершину?

А) Одно событие влечет за собой другое событие

Б) Использование описания одной рутины для одинаковых по функционированию периферийных узлов

В) действия, описанные в событийной секции, выполняются мгновенно

2. Какое название получила технология использования глобальной сети компьютеров для решения сложной задачи

А) Grid

Б) Site

В) Web

3. Под степенью отношения понимается...

А) количество атрибутов

Б) количество кортежей

В) количество строк

3. С помощью какого алгоритма производится поиск идентификатора с наибольшей оценкой

А) децентрализованного алгоритма

Б) алгоритма смещения

В) алгоритма Тарри

4. В каком слое отсутствует описание связей между узлами

А) сообщений

Б) структуры

В) алгоритмов

5. Назовите основные задачи РРИСО

А) интеграция с аналоговыми информационными системами

Б) совместное использование вычислительных ресурсов защита информации

6. Какую структуру имеет объект автоматизации

А) географически распределенную структуру

Б) региональную структуру

В) географически сосредоточенную структуру

7. Подсистема подготовки и принятия решений использует информацию, получаемую из.

А) подсистемы мониторинга

Б) хранилища РРИСО

В) подсистемы внутреннего документооборота

8. В каком случае возникает вертикальная фрагментация

А) по различным сайтам распределена информация о различных сущностях предметной области

Б) источники данных и пользователи привязаны к сайтам, находящимся в различных точках физического пространства, а реляционные схемы, которыми они пользуются, могут быть одинаковы

В) об одних и тех же сущностях на разных сайтах имеется информация разного рода

9. Для чего необходимо вести централизованную базу данных РРИСО

А) для обеспечения управления системой

Б) для формирования типовых документов

В) для обеспечения единого интерфейса пользователя

10. К репликации можно отнести

А)создание копий некоторых фрагментов отношений

Б) одновременное хранение нескольких копий на разных сайтах

В) повышение надежности хранения данных

10. В каком алгоритме каждый инициатор вычисляет список идентификаторов всех инициаторов

А) алгоритм Тарри

Б) алгоритм Чанга-Робертса

В) алгоритм Лелана

7.2.4 Примерный перечень вопросов для подготовки к зачету с оценкой

1.Понятие распределенной системы. Определение распределенной системы. Особенности распределенных систем. Примеры и применения

2.Параллельные и распределенные системы. Сравнение параллельных и распределенных систем. Области применения

3.Архитектурные особенности. Сервисы, роли и архитектурные стили. Клиент-серверная архитектура. Одноранговые сети (P2P)

4.Сервисно-ориентированная архитектура (SOA).

5.Дизайн масштабируемых распределенных систем. Понятие масштабируемости. Особенности проектирования распределенных систем

6. Введение в моделирование. Понятие модели. Модель распределенного исполнения. Модель коммуникационного канала

7.Событийное описание. Упорядочивание событий. Отношение причинного предшествования.

8.Логическое время. Отметки времени Лампорта.

9.Реализация логических часов. Скалярное время. Векторное время. Алгоритмы реализации векторных часов

10.Синхронное и асинхронное исполнение. Характеристики режимов. Эмуляции синхронных систем асинхронными и наоборот

11.Модели отказов. Отказы процессов. Отказы коммуникационных каналов. Иерархия моделей неисправности

12.Свойства распределенных алгоритмов.

13.Глобальное состояние. Распределенная сборка мусора. Распределенное обнаружение тупиков. Распределенное обнаружение завершения.

Фиксация глобального состояния

14.Введение и состав коммуникационной подсистемы. Сети и сетевые технологии

15.Ключевые проблемы использования сетей в распределенных системах. Принципы построения сетей

16.Маршрутизация и алгоритмы на графах. Алгоритмы маршрутизации

17.Межпроцессный обмен. Особенности обмена сообщениями. Адресация. Широковещательные рассылки (broadcast). Многоадресные рассылки (multicast)

18. Удаленные вызовы. Протокол «запрос-ответ» (request-reply). Удаленный вызов процедуры (RPC). Пример удаленного вызова — веб-сервисы

19. Косвенные (indirect) коммуникации. Очереди сообщений.

20. Групповые коммуникации. Координация и согласие в групповых коммуникациях. Базовые многоадресные рассылки. Надежная многоадресная рассылка.

21. Упорядоченные многоадресные рассылки. Открытые группы и виртуальная синхронность

22. Введение в синхронизацию. Алгоритмы синхронизации часов. Алгоритм Кристиана. Алгоритм Беркли

23. Усредняющие алгоритмы.

24. Алгоритмы выбора (лидера)

25. Распределенное взаимоисключение

26. Введение в проблему консенсуса. Модель системы и основные определения. Согласие в системах с отказами

27. Отсутствие детерминированного решения в асинхронных системах (FLP impossibility). Способы обхода результата FLP impossibility

28. Алгоритм PAXOS. Распределенные транзакции

29. Типы транзакций. Компоненты архитектуры для поддержки распределенных транзакций. Управление параллельным выполнением транзакций

30. Метод временных меток. Контроль параллельного исполнения транзакций.

31. Протоколы распределенного завершения (2PC, 3PC)

32. Восстановление после отказов

33. Введение в репликацию. Модель и архитектура управления реплицированными данными. Пассивная и активная репликация

34. Отказоустойчивость сервиса репликации. Модели консистентности.

35. Модели непротиворечивости, ориентированные на данные.

36. Модели непротиворечивости, ориентированные на клиента

37. Протоколы кворума

38. Введение в распределенное хранение. Современные подходы к построению систем распределенного хранения. Программно-определяемые хранилища. Механизм хранения данных на уровне объектов

39. Архитектурные особенности

40. Пиринговые системы (P2P). Безопасность P2P-сетей

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Технологии и платформы распределённой обработки данных. Apache Hadoop. Архитектура и основные концепции
2. Технологии и платформы распределённой обработки данных. Apache Spark. Архитектура и основные концепции
3. Контейерные технологии и платформы. Docker: архитектура, образы, контейнеры
4. Контейерные технологии и платформы. Kubernetes. Платформа оркестрации контейнеров. Основные компоненты Kubernetes
5. Облачные вычисления. Модели развертывания. Частное облако (Private Cloud). Публичное облако (Public Cloud). Общественное облако (Community Cloud). Гибридное облако (Hybrid Cloud)
6. Модели обслуживания. SaaS (Software as a Service), PaaS, IaaS
7. АРХИТЕКТУРНЫЕ ШАБЛОНЫ (ПАТТЕРНЫ) ПРОЕКТИРОВАНИЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ. Одноузловые паттерны проектирования.
8. Паттерн Sidecar. Пример реализации паттерна Sidecar (добавление HTTPS к унаследованному сервису). Динамическая конфигурация с помощью паттерна Sidecar.
9. Паттерн Ambassador. Использование для шардирования сервиса
10. Паттерны проектирования обслуживающих систем
11. Функции и событийно-ориентированная обработка
12. Паттерны FaaS (Functions as a Service)
13. Событийно-ориентированная пакетная обработка
14. Паттерны событийно-ориентированной обработки. Паттерн Copier (копировщик). Паттерн Filter (фильтр).
15. Паттерны событийно-ориентированной обработки.Паттерн Splitter (разделитель). Паттерн Sharder (шардировщик). Паттерн Merger (объединитель)
16. Особенности реализации информационной безопасности в озере данных Hadoop
17. Специфические угрозы информационной безопасности в озере данных
18. Организационные меры по информационной безопасности для озера данных
19. Обзор подсистем безопасности озера данных
20. Безопасные протоколы. Kerberos. Шифрование SSL/TLS
21. Инструменты безопасности Hadoop. Использование шлюза безопасности Apache Knox Gateway
22. Инструменты безопасности Hadoop. Политики разграничения доступа Apache Ranger
23. Защита данных HDFS. Шифрование данных при передаче. SSL шифрование для подключения к WebUI компонент экосистемы Hadoop
24. Управление доступом к HDFS. Антивирусная защита в озере данных
25. Безопасность Docker. Обеспечение безопасности контейнеров на базе Docker. Принцип минимальных привилегий

26. Безопасность Docker. Обеспечение безопасности identidock (пример).

27. Безопасность Docker. Подтверждение происхождения образов. Механизм подтверждения контента в Docker (Content Trust).

28 Безопасность Docker. Обеспечение безопасной загрузки ПО в файлах Dockerfile. Рекомендации по обеспечению безопасности

29. Безопасность Kubernetes. Защита сервера API Kubernetes. Аутентификация. RBAC (Role-Based Access Control) — защита кластера

30. Основы безопасности облачных вычислений. Границы безопасности. Модель стека Cloud Security Alliance (CSA)

31. Управление доступом в облаке. Контроль доступа. Аутентификация. Авторизация

32. Изолированный доступ к данным

33. Brokered Cloud Storage Access (брокерский доступ к облачному хранилищу)

34. Работа брокерской облачной системы доступа к хранилищу

35. Шифрование в облаке

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится в форме тестирования с практическим заданием. Каждый зачетный билет (вариант) содержит: 10 тестовых вопросов (каждый правильный ответ — 1 балл).

Максимальное количество баллов за зачет 10 (тесты) = 10 баллов

Шкала оценивания

Оценка	Традиционная шкала	Количество баллов
«Зачтено»	Отлично	9–10 баллов
«Зачтено»	Хорошо	7–8 баллов
«Зачтено»	Удовлетворительно	4–6 баллов
«Не зачтено»	Неудовлетворительно	менее 3 баллов

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов - 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в распределённые системы	ПК-4.5	Тест, защита лабораторных работ
2	Проектирование РИС	ПК-4.5	Тест, защита лабораторных работ
3	Безопасность РИС	ПК-4.5	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Бабичев, С. Л. Распределенные системы: учебник для вузов / С. Л. Бабичев, К. А. Коньков. — Москва: Издательство Юрайт, 2026. — 507 с. — (Высшее образование). — ISBN 978-5-534-11380-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. —

URL: https://urait.ru/bcode/587607

Технологии обеспечения информационной безопасности больших данных в компьютерных сетях. Информационная безопасность в системах обработки данных на примере Hadoop и Spark: учебно-методическое пособие / составители А. В. Осин, К. А. Хализев. — Москва: МТУСИ, 2025. — 18 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/501212

Дополнительная литература

Северцев, Н. А. Динамические системы: безопасность и отказоустойчивость: учебное пособие для вузов / Н. А. Северцев. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-05711-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493435

Перрен, Ж. -. Spark в действии / Ж. -. Перрен; перевод с английского А. В. Снастина. — Москва: ДМК Пресс, 2021. — 636 с. — ISBN 978-5-97060-879-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/241001

Бутаков, Н. А. Обработка больших данных с Apache Spark: учебно-методическое пособие / Н. А. Бутаков, М. В. Петров, Д. Насонов. — Санкт-Петербург: НИУ ИТМО, 2019. — 50 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/136573

Годзурас, Э. Docker Compose для разработчика: руководство / Э. Годзурас ; перевод с английского А. Н. Киселева. — Москва: ДМК Пресс, 2023. — 220 с. — ISBN 978-5-93700-203-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/348110

Вьяс, Д. Kubernetes изнутри / Д. Вьяс, К. Лав; перевод с английского А. Н. Киселева. — Москва : ДМК Пресс, 2023. — 378 с. — ISBN 978-5-93700-153-5. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/314942.

Аймен, Э. А. Облачные микросервисы в Kubernetes: руководство / Э. А. Аймен; пер. с англ. В. С. Яценкова. — Москва : ДМК Пресс, 2025. — 276 с. — ISBN 978-5-93700-324-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/514873

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Классические материалы

Distributed Systems (Курс Мартина Клеппмана)

https://martin.kleppmann.com/2020/11/18/distributed-systems-3rd-edition.html

The CAP Theorem (теорема CAP)
https://www.julianbrowne.com/article/brewers-cap-theorem
FLP Impossibility Result
https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf
Алгоритмы и протоколы
Paxos Algorithm (алгоритм консенсуса)
https://lamport.azurewebsites.net/pubs/paxos-simple.pdf
Raft Consensus Algorithm
https://raft.github.io
Raft Visualizer (интерактивная визуализация)
http://thesecretlivesofdata.com/raft
Распределенные транзакции
Two-Phase Commit (2PC)
https://www.microsoft.com/en-us/research/publication/consensus-protocols-two-phase-commit
Документация по ACID https://databass.dev
Официальный сайт Hadoop
https://hadoop.apache.org
Документация HDFS (Hadoop Distributed File System)
https://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-hdfs/HdfsDesign.html
Документация MapReduce
https://hadoop.apache.org/docs/stable/hadoop-mapreduce-client/hadoop-mapreduce-client-core/MapReduceTutorial.html
Официальный сайт Docker
https://www.docker.com
Документация Docker
https://docs.docker.com
Docker Hub (реестр образов)
https://hub.docker.com
Официальный сайт Kubernetes
https://kubernetes.io
Документация Kubernetes
https://kubernetes.io/docs/home
Интерактивный тур по Kubernetes
https://kubernetes.io/docs/tutorials/kubernetes-basics

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Безопасность распределенных компьютерных систем» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения;

	- участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4