АННОТАЦИЯ

к рабочей программе дисциплины

«Безопасность распределенных информационных систем»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Цель изучения дисциплины: является формирование целостного представления об организации информационной безопасности распределённых информационных систем, получение теоретических знаний о принципах построения и архитектуре подобных систем.

Задачи изучения 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

Содержание дисциплины:

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 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; рас-

пределенное 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

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. 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

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 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. Шифрование

Перечень формируемых компетенций:

ПК-7.4 - Способен оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите

Общая трудоемкость дисциплины: 8 з.е.

Форма итогового контроля по дисциплине: Экзамен