2023 г. **Бакалавриат ПМиИ**

Вопросы для подготовки к государственному экзамену (дополнительная часть)

Кафедра информационной безопасности (группа 419/2)

1. Функции алгебры логики. Критерий полноты системы функций алгебры логики.
2. Функции k-значных логик. Теоремы о представимости функций k-значных логик 1-й и 2-й формами. Теорема о представимости функций k-значных логик полиномами по модулю k.
3. Ограниченно-детерминированные (о.-д.) функции. Операции суперпозиции и обратной связи над ними. Конечная порожденность класса о.-д. функций относительно этих операций.
4. Алфавитное кодирование. Алгоритм распознавания однозначности алфавитного кодирования.
5. Эквивалентные преобразования в функциональных системах. Конечные полные системы тождеств для формул алгебры логики и схем из функциональных элементов.
6. Дизъюнктивные нормальные формы (ДНФ). Сокращенные, тупиковые, минимальные ДНФ, алгоритмы их построения. Оценки сложности ДНФ.
7. Схемы из функциональных элементов. Метод Лупанова для синтеза схем из функциональных элементов.
8. Сложность алгоритмов. Классы P и NP. Теорема об NP-полноте задачи о выполнимости КНФ.
9. Независимые случайные величины. Критерий независимости случайных величин.
10. Моменты случайных величин. Свойства математических ожиданий и дисперсий.
11. Центральная предельная теорема.
12. Точечные и интервальные оценки неизвестных параметров распределений. Свойства точечных оценок (несмещенность, состоятельность, эффективность, оптимальность). Два метода построения точечных оценок (метод максимального правдоподобия, метод моментов).
13. Основные понятия о проверке статистических гипотез. Лемма Неймана-Пирсона.
14. Доверительные интервалы для параметров нормального распределения.
15. Виды сходимостей последовательностей случайных величин.
16. Виды параллельной обработки данных. Компьютеры с общей и распределенной памятью.
17. Производительность вычислительных систем, методы оценки и измерения.
18. Закон Амдала, его следствия. Этапы решения задач на параллельных вычислительных системах. Граф алгоритма, критический путь графа алгоритм, ярусно-параллельная форма графа алгоритма.
19. Основные задачи обеспечения информационной безопасности. Понятия угрозы, уязвимости, атаки. Модель нарушителя. Архитектура фон-Неймана и Гарвардская архитектура с точки зрения информационной безопасности. Уязвимости внедрения кода, основные причины их появления, примеры. Формирование требований к ИБ в контексте цикла безопасной разработки программного обеспечения. Моделирование угроз.
20. Валидация структурных типов входных данных веб-приложений. Валидация загружаемых файлов. Возможные ошибки и угрозы защищенности. Защищенная реализация загрузки файла по URL-адресу, полученному от пользователя; SSRF.
21. Структура виртуальной памяти процесса в современных операционных системах. Структура исполнимого файла в формате ELF. Связь структуры исполнимого файла и памяти процесса. Ошибки порчи памяти с примерами: переполнение стека, форматная строка в Си, переполнение кучи, целочисленное переполнение. Механизмы защиты от ошибок порчи памяти уровня операционной системы и процессора.
22. Организация кучи в современных операционных системах, аллокаторы. Устройство кучи на примерах dlmalloc и ptmalloc. Примеры уязвимостей переполнения кучи и атак на переполнение кучи. Эксплуатация уязвимости переполнения кучи через Unlink()
23. Понятие аутентификации и авторизации субъектов информационного взаимодействия. Модели управления доступом RBAC и ABAC. Ошибки авторизации. Аутентификация и авторизация пользователей в микросервисной архитектуре - варианты реализации и их свойства. Взаимная аутентификация и авторизация микросервисов - постановка задачи и варианты реализации.

24. Особенность использования криптографических примитивов для хранения пользовательских паролей, KDF для хранения паролей, специальные KDF для затруднения переборных атак на пароли.
25. Безопасность сетевых протоколов. Атаки амплификации с примерами: DNS, NTP amplification. Причины уязвимости протоколов к атакам амплификации. Способы защиты.
26. Два способа построения архитектуры сетевого приложения - централизованный и децентрализованный. CDN и IP Anycast для централизованных приложений. DHT и примеры.
27. Атаки класса “отказ в обслуживании” с примерами. Механизмы защиты от атак на отказ в обслуживании: фильтрация на уровне сети (центры очистки и механизмы их организации), на уровне канала, на уровне операционной системы. Механизм TCP syncookie.
28. Защищенность мобильных устройств и приложений. Архитектура платформы Android, компонентный состав ПО на мобильном устройстве под управлением Android. Цели и способы воздействия на мобильное устройство и компоненты его ПО. Решения уровня платформы, обеспечивающие защиту устройства, системного ПО, прикладного ПО и данных пользователя.
29. Схема защищенной аутентификации пользователей онлайн-сервиса в мобильном приложении. Схема первичной привязки мобильного приложения к устройству, схема упрощенной аутентификации через PIN-код и биометрические данные. Обсуждение свойств защищенности схем.
30. Принципы построения защищенной архитектуры. Принцип Zero Trust.
31. Внешние и внутренние компоненты кода. Угрозы при их использовании и меры защиты от этих угроз. Выбор технологии реализации: самостоятельная реализация или готовая внешняя компонента.
32. Место информационной безопасности в жизненном цикле ПО. McGraw’s Touchpoints. Microsoft SDL.
33. Частично упорядоченные множества и решетки: определение, свойства, характеристики, операции над ними, важные элементы, изоморфизм. Диаграмма Хассе. Конструкторы решеток: плоская решетка, показательная решетка, прямое произведение и степень, функциональная решетка. Монотонные функции на решетках. Композиция монотонных функций. Теорема Клини о неподвижной точке. Наивный алгоритм поиска неподвижной точки и его вычислительная сложность.
34. Абстрактная интерпретация. Абстрактные домены. Соотношение Галуа. Граф потока управления и алгоритм его построения для последовательных императивных программ. Монотонные фреймворки на примере анализа знаков, анализа распространения констант и анализа ограниченных перечислений.
35. Монотонный фреймворк в интервальном домене: арифметика и сравнения. Расширение и сужение.
36. Парадигма функционального программирования. Основные концепции, принципы, накладываемые ограничения. Теоретико-множественное определение функции. Чистое нетипизированное λ-исчисление: синтаксис и семантика. Нормализация, стратегии редукции. Теорема Черча-Россера (без доказательства). Рекурсия и комбинатор неподвижной точки. Кодирование по Черчу. Каррирование, частичное применение. η-конверсия, композиция функций, бесточечная нотация.
37. Парадигма объектно-ориентированного программирования. Основные концепции, принципы, накладываемые ограничения. Принципы построения объектной модели. Основные элементы и определения. Виды связей. Основной вид деятельности в объектно-ориентированной разработке. Контрактное программирование. Принципы SOLID. Определения, контекст применения, примеры.
38. Системы типов и эффектов: определение, таксономия, примеры. Алгебраические типы данных. Изоморфизм типов. Expression problem. Классификация видов полиморфизма по Карделли и Вегнеру, варианты реализаций этих видов полиморфизма в различных языках программирования. Рядовой полиморфизм. Вариантность. Варианты обработки ошибок и исключительных ситуаций в широком смысле (значения, исключения).
39. Моделирование предметной области. Единый язык, подобласти, ограниченные контексты, карта контекстов. Методы моделирования. Тактические шаблоны предметно-ориентированного проектирования, примеры использования. Различие между анемичной и богатой моделью предметной области. Архитектурные шаблоны. Многоуровневая архитектура, основанная на инверсии зависимостей: основные уровни, их ответственность, возможные направления зависимостей. Архитектура портов и адаптеров.

Литература

1. Яблонский С.В. Введение в дискретную математику. -М.: Высшая школа, 2001.
2. Алексеев В.Б. Лекции по дискретной математике. М.: ИНФРА-М, 2012.
3. Яблонский С.В. Элементы математической кибернетики. М.: Высшая школа, 2007.
4. Сапоженко А.А. Некоторые вопросы сложности алгоритмов. М.: Изд-во ф-та ВМК, 2001.
5. Феллер В. Введение в теорию вероятностей и ее приложения, т.1, т.2. -М.: Либроком, 2010.
6. Ивченко Г.И., Медведев Ю.И. Математическая статистика.-М.: Либроком, 2014.
7. В.В.Воеводин, Вл.В.Воеводин. "Параллельные вычисления", БХВ-Петербург, 2002, 608 стр.
8. Zalewski, Michal. The tangled Web: A guide to securing modern web applications. No Starch Press, 2012.
9. Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte. The Shellcoder's Handbook: Discovering and Exploiting Security Holes.
10. Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Detecting and Exploiting Security Flaws.
11. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse. The Mobile Application Hacker's Handbook.
12. Michael Howard, Steve Lipner. Security Development Lifecycle
13. John Vega, Gary McGraw. Building Secure Software
14. Gary McGraw. Software Security: Building Security In
15. Вигерс Карл И., Битти Джой. Разработка требований к программному обеспечению.
16. Møller, A., Schwartzbach, M. I. Static Program Analysis. 2022.
17. Pierce B. Types and Programming Languages. The MIT Press, 2002.
18. Мейер Б. Объектно-ориентированное конструирование программных систем. 2005.
19. Мартин Р. Чистая архитектура. Искусство разработки программного обеспечения. Питер, 2022.
20. Эванс Э. Предметно-ориентированное проектирование: структуризация сложных программных систем. Вильямс, 2020.
21. Вернон В. Реализация методов предметно-ориентированного проектирования. Диалектика-Вильямс, 2019.