Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное учреждение науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
(ИСП РАН)

Одобрено решением учёного совета ИСП РАН **Протокол № 2022-8 от 14 июня 2022 г.**	**«УТВЕРЖДАЮ»** **Директор ИСП РАН** **д.ф.-м.н., академик РАН** **_____А.И. Аветисян** **«14» июня 2022 г.**

ПРОГРАММА

ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА В АСПИРАНТУРУ

по специальности

1.2.4 - Кибербезопасность

Москва 2022

1. Математические основы кибербезопасности

1.1. Основные понятия теории алгоритмов. Машины Тьюринга. Нормальные алгоритмы Маркова. Понятия об алгоритмической неразрешимости.

1.2. Структуры данных. Множества, полная упорядоченность, индексация. Графы и деревья, обход деревьев. Стеки, очереди. Массивы. Списки (одинарные, двойные). Доступ к данным, включение и исключение элементов данных. Представление в памяти ЭВМ различных структур данных: графов, деревьев, стеков, очередей.

2. Вычислительные машины и сети ЭВМ

2.3. Архитектура ЭВМ, организация процессора. Оперативная и внешняя память. Представление команд и данных в ЭВМ. Устройства ввода и вывода информации. Параллелизм работы устройств ЭВМ, таксономия Флинна.

2.4. Организация аппаратного обеспечения компьютера. Технологии разработки и производства интегральных схем, этапы разработки и технические средства. Эмпирические законы развития ЭВМ. Классы вычислительных систем: процессоры общего назначения, микроконтроллеры, программируемая интегральная логическая схема, интегральные схемы специального назначения.

2.5. Многозадачная работа компьютера: требования к аппаратуре. Пользовательский и привилегированный режимы работы ЦПУ. Аппарат защиты памяти: сегменты, страничная организация, TLB. Прерывания. Системные вызовы.

2.6. Процессы. Реализация процессов. Взаимодействие процессов. Параллельные процессы. Взаимное исключение и взаимная синхронизация. Примитивы синхронизации: события, семафоры, мониторы Хоара, почтовые ящики.

2.7. Распределение времени процессора. Мультипрограммирование. Методы планирования в мультипрограммных системах.

2.8. Управление памятью. Распределение памяти и организация доступа к памяти в ЭВМ с различной структурой памяти. Виртуальная память. Стратегии и методы замещения страниц.

2.9. Программное обеспечение сетей ЭВМ. Базовая эталонная модель взаимодействия открытых систем.

3. Методы компиляции и статического анализа

3.1. Языки и грамматики. Синтаксис и семантика языков программирования. Формальное определение грамматики и языка. Классификации грамматик по Хомскому.

3.2. Ассемблеры и загрузчики. Команды и псевдокоманды, символические адреса, адресные выражения. Организация работы двухпроходного ассемблера. Классификация загрузчиков и методы загрузки.

3.3. Основные этапы работы компилятора: лексический анализ, синтаксический анализ и генерация промежуточного кода, генерация объектного кода, оптимизация кода.

3.4. Лексический анализатор. Синтаксический разбор. Нисходящий анализ, метод рекурсивного спуска. Восходящий анализ. Грамматика предшествования.
3.5. Структура оптимизирующего компилятора. Типы промежуточного представления. Базовые блоки и граф потока управления программы. Алгоритм выделения базовых блоков и построения графа потока управления.
3.6. Структура потока данных и общий итерационный алгоритм анализа потока данных. Монотонные и дистрибутивные структуры потока данных.
3.7. Простые машинно-независимые оптимизирующие преобразования: алгебраические упрощения, сворачивание констант, распространение копий.
3.8. SSA-форма. Алгоритм построения максимальной SSA-формы. Восстановление кода из SSA-формы. Замена φ-функций группами инструкций копирования.
3.9. Применения статического анализа. Актуальность поиска ошибок в программах, возможные методы. Понятия статического и динамического анализа программ. Ошибки, допускаемые анализатором. Выделение ошибочных ситуаций, причины появления различных ситуаций для одного класса ошибок.

4. Методы динамического анализа программ, методы анализа бинарного кода и исследований для поиска уязвимостей

4.1. Применение отладки для оценки возможности эксплуатации уязвимостей. Технологии отладки. Отладка пользовательского кода. Полносистемная отладка в виртуальной машине.
4.2. Форматы исполняемых и объектных файлов на примере ELF. Секции и сегменты. Таблицы символов и перемещений. Статическая компоновка. PIC и PIE: способы организации.
4.3. Динамическая двоичная трансляция. Инфраструктура Valgrind. Инструмент memcheck пакета Valgrind.
4.4. Инструментирование исходного кода программ в процессе компиляции. Инструменты-санитайзеры в компиляторах GCC и LLVM. Address Sanitizer, Memory Sanitizer, Thread Sanitizer.
4.5. Фаззинг: определение, применение, принципы. Схема инструмента. Разновидности фаззинга: черный ящик, белый ящик, серый ящик. Генетические алгоритмы в фаззинге.

5. Методы конструирования доверенных программных и программно-аппаратных систем

5.1. Методологии разработки безопасного ПО: Microsoft SDL, CSDL, BSIMM, OWASP SAMM. Оценка зрелости жизненного цикла безопасного ПО.
5.2. Система национальных стандартов разработки безопасного ПО, ГОСТ Р 56939.
5.3. Технологии анализа кода, применяемые в жизненном цикле безопасного ПО, и требования, предъявляемые к ним.

6. Методы синтеза и верификации цифровой аппаратуры

6.1. Маршрут проектирования цифровой аппаратуры. Уровни представления аппаратуры. Логический и физический синтез. Верификация и ее разновидности. Специфика маршрута проектирования для ПЛИС (FPGA) и заказных СБИС (ASIC).

6.2. Язык описания аппаратуры Verilog. Основные конструкции языка: модули, экземпляры модулей, управляющие операторы, непрерывное и процедурное присваивание, always-блоки. Операционная семантика (модель исполнения). Синтез логической схемы по Verilog-описанию.

6.3. Основные комбинационные и последовательные схемы. Шифраторы, дешифраторы. Мультиплексоры, демультиплексоры, селекторы. Сумматоры, компараторы. Счетчики, сдвиговые регистры. Очереди, блоки памяти прямого доступа. Конечные автоматы, конвейеры.

6.4. Организация ПЛИС. Мелко-, средне- и крупноблочные архитектуры. Таблицы соответствия (LUT), конфигурируемые логические блоки (CLB), блоки логических массивов (LAB). Встроенные блоки памяти (BRAM) и встроенные вычислительные блоки (DSP). Конфигурирование ПЛИС.

7. Верификация программных и программно-аппаратных систем

7.1. Формализация семантики языков программирования. Операционная и аксиоматическая семантика. Частичная и полная корректность программы. Понятия инварианта цикла, слабейшего предусловия, сильнейшего постусловия.

7.2. Методы Флойда верификации программ: метод индуктивных утверждений, метод фундированных множеств. Построение условий верификации и условий завершимости.

7.3. Темпоральная логика линейного времени (LTL). Размеченные системы переходов. Интерпретация формул LTL на траекториях систем переходов. Свойства безопасности и живости. Понятие справедливости планировщика.

7.4. Автоматы Бюхи и регулярные (автоматные) □-языки. Проверка автоматного языка на пустоту. Распознавание пересечения автоматных языков. Алгоритм построения автомата Бюхи по формуле LTL. Теоретико-автоматный подход к проверке моделей (model checking).

8. Методы интеллектуального анализа данных

8.1. Нейрон и нейронная сеть. Задачи, решаемые при помощи нейронных сетей.

8.2. Компоненты нейронной сети. Методы оптимизации. Сверточные нейронные сети.

8.3. Регуляризация, нормализация и метод максимального правдоподобия. Методы ускорения классификации при помощи нейросетей.

8.4. Естественный язык и текст. Векторная модель текста и классификация длинных текстов. Классификация новостных текстов.

8.5. Базовые методы работы с текстом при помощи нейронных сетей. Классификация коротких текстов. Распознавание структуры коротких текстов. Распознавание именованных сущностей.

Литература

1. Ахо,Лам,Сети,Ульман. Компиляторы. Принципы, технологии, инструменты. М., 2008, 2изд.
2. Cooper K., Torczon L. Engineering a Compiler, Second Edition.2011.
3. Flemming Nielson, Hanne R. Nielson, Chris Hankin. Principles of Program Analysis / Springer, 1999
4. Al Bessey, Ken Block, Ben Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, Dawson Engler. A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World // Comunications of the ACM, 2010, vol. 53, no. 2, pp. 66-75.
5. Brian Chess, Jacob West. Secure Programming with Static Analysis / Addison-Wesley Professional, 2007.
6. Nethercote N., Seward J. Valgrind: a framework for heavyweight dynamic binary instrumentation // ACM Sigplan notices. – ACM, 2007. – Т. 42. – №. 6. – С. 89-100.
7. Амини П., Саттон М., Грин А. Fuzzing: исследование уязвимостей методом грубой силы. — Символ-Плюс, 2009.
8. Edward J. Schwartz, Thanassis Avgerinos, David Brumley. All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask), 2010
9. В.А. Падарян, А.И. Гетьман, М.А. Соловьев, М.Г. Бакулин, А.И. Борзилов, В.В. Каушан, И.Н. Ледовских, Ю.В. Маркин, С.С. Панасенко. Методы и программные средства, поддерживающие комбинированный анализ бинарного кода // Труды Института системного программирования РАН Том 26. Выпуск 1. - 2014 г. - С. 251-276
10. Balakrishnan G., Reps T. Analyzing memory accesses in x86 executables // International conference on compiler construction. – Springer Berlin Heidelberg, 2004. – С. 5-23 (https://research.cs.wisc.edu/wpis/papers/cc04.pdf)
11. M. Handley, V. Paxson. Network Intrusion Detection: Evasion Traffic Normalization And End-to-End Protocol Semantics//Proceedings of the 10th USENIX Security Symposium. - 2001.
12. Методика оценки угроз безопасности информации. ФСТЭК России. https://fstec.ru/tekhnicheskaya-zashchitainformatsii/dokumenty/114-spetsialnyenormativnye-dokumenty/2170-metodicheskij-dokument-utverzhdenfstek-rossii-5-fevralya-2021-g
13. Таненбаум Э., Уэзеролл Д. «Компьютерные сети». 5 издание. Питер, 2022.
14. Justin Schuh, John McDonald, Mark Dowd. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. 2006.
15. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 2014.

16. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2007
17. Tobias Klein. A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security. 2011.
18. Ian Goodfellow, Yoshua Bengio, and Aaron Courville. 2016. Deep Learning. The MIT Press.
19. Christopher M. Bishop. 2006. Pattern Recognition and Machine Learning (Information Science and Statistics). Springer-Verlag, Berlin, Heidelberg.
20. Sebastian Raschka. 2015. Python Machine Learning. Packt Publishing.
21. Daniel Jurafsky and James H. Martin. 2009. Speech and Language Processing (2nd Edition). Prentice-Hall, Inc., Upper Saddle River, NJ, USA.
22. К.А. Коньков, В.Е. Карпов Основы операционных систем. М.: Интернет университет информационных технологий. 2004.
23. Таненбаум Э. Современные операционные системы. - СПб.: Питер, 2002.
24. Рэндал Э. Брайант, Дэвид О'Халларон. Компьютерные системы: архитектура и программирование (Computer Systems: A Programmer's Perspective). Издательство: БХВ-Петербург, 2005 г. — 1186 стр.
25. Д.В. Буздалов, Е.В. Корныхин, А.А. Панфёров, А.К. Петренко, А.В. Хорошилов. Практикум по дедуктивной верификации программ: учебно-методическое пособие. М: МАКС Пресс, 2014.
26. А.С. Камкин. Введение в формальные методы верификации программ: учебное пособие. М: МАКС Пресс, 2018.
27. Ю.Г. Карпов. Model Checking. Верификация параллельных и распределенных программных систем. БХВ-Петербург, 2010.
28. K.R. Apt, F.S. de Boer, E.-R. Olderog. Verification of Sequential and Concurrent Programs. Springer, 2009.
29. C. Baier, J.-P. Katoen. Principles of Model Checking. The MIT Press, 2008.
30. M. Ben-Ari. Mathematical Logic for Computer Science. Springer, 2012.
31. Цифровой синтез: практический курс / под общ. ред. А.Ю. Романова, Ю.В. Панчула. М.: ДМК Пресс, 2020.
32. S. Bhunia, M. Tehranipoor. Hardware Security A Hands-on Learning Approach. Morgan Kaufmann, 2019.
33. Д. Харис, С. Харис. Цифровая схемотехника и архитектура компьютера: RISC-V. М.: ДМК Пресс, 2021.
34. К. Максфилд. Проектирование на ПЛИС. Архитектура, средства и методы. Курс молодого бойца. М.: Додэка XXI, ДМК Пресс, 2015.
35. Web Application Security A Beginner's Guide. Bryan Sullivan, Vincent Liu. 2011
36. Основные понятия PKI. http://www.cryptocom.ru/articles/pki.html
37. Ключи, шифры, сообщения: как работает TLS. А. Венедюхин. https://tls.dxdt.ru/tls.html