2026 г. **Бакалавриат ПМиИ**

Вопросы для подготовки к государственному экзамену (дополнительная часть)

Кафедра информационной безопасности (гр. 491)

1. Функции алгебры логики. Критерий полноты системы функций алгебры логики.
2. Графы, деревья. Свойства деревьев. Планарные графы. Формула Эйлера для планарных графов. Критерий Понтрягина-Куратовского (доказательство в одну сторону).
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. Сводимость по Куку, сводимость по Карпу, замкнутость класса NP относительно сводимости по Карпу (с доказательством), понятие «самосводимости».
10. Вероятностная машина Тьюринга, классы сложности RP, coRP, BPP, известные соотношение между ними (с доказательствами), принцип амплификации.
11. Независимые случайные величины. Критерий независимости случайных величин.
12. Моменты случайных величин. Свойства математических ожиданий и дисперсий.
13. Центральная предельная теорема.
14. Точечные и интервальные оценки неизвестных параметров распределений. Свойства точечных оценок (несмещенность, состоятельность, эффективность, оптимальность). Два метода построения точечных оценок (метод максимального правдоподобия, метод моментов).
15. Основные понятия о проверке статистических гипотез. Лемма Неймана-Пирсона.
16. Доверительные интервалы для параметров нормального распределения.
17. Основная теорема матричных игр.
18. Выпуклые множества и выпуклые функции. Необходимое и достаточное условие оптимальности в общей задаче оптимизации.
19. Конечные поля. Теорема о том, что мультипликативная группа поля является циклической. Малая теорема Ферма для конечных полей. Примитивный элемент.
20. Линейные регистры сдвига (ЛРП) над конечными полями. Присоединенный многочлен ЛРП. Теорема о периоде ЛРП, у которого присоединенный многочлен является примитивным.
21. Теорема Мак-Элиса о делимости веса булевой функции на степень 2.
22. Теорема о числе булевых функций, имеющих тривиальную группу инерции в полной аффинной группе.
23. Матричные критерии для бент – функций.
24. Теорема Зигенталера о верхней границе алгебраической степени корреляционно–иммунных и устойчивых функций.
25. Теорема о верхней границе для порядка алгебраической иммунности булевой функции.
26. Определение криптографической хэш-функции, ее основные приложения. Задача о днях рождения. Однородная и неоднородная схемы размещения шаров по ящикам. Оценки вероятности попадания двух и более шаров в один ящик для однородной схемы. Атака на структуру Меркла-Дамгора типа «встреча посередине».
27. Структура Меркла–Дамгора. Атака корректировкой блока и атака с использованием неподвижных точек. Хэш-функции на основе блочных шифров: общий вид и уязвимости.
28. Определение кода аутентификации, его табличное представление и основные приложения. Атаки имитации и подмены, свойства их вероятностей. Оптимальные коды аутентификации.
29. Криптосистема RSA, доказательство однозначности расшифрования в этой криптосистеме. Слепая подпись RSA.
30. Протокол электронной подписи. Протокол подписи Рабина, доказательство его стойкости.
31. Виды параллельной обработки данных. Компьютеры с общей и распределенной памятью. Производительность вычислительных систем, методы оценки и измерения.
32. Закон Амдала, его следствия. Этапы решения задач на параллельных вычислительных системах. Граф алгоритма, критический путь графа алгоритм, ярусно-параллельная форма графа алгоритма.

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] Марченков С.С. Избранные главы дискретной математики. М.: МАКС Пресс, 2015.
[6] Феллер В. Введение в теорию вероятностей и ее приложения,т.1, т.2. -М.: Либроком, 2010.
[7] Ивченко Г.И., Медведев Ю.И. Математическая статистика.-М.: Либроком, 2014.
[8] Гермейер Ю.Б. Введение в теорию исследования операций.-М.: Наука, 1971.
[9] Сухарев А.Г., Тимохов А.В., Федоров В.В. Курс методов оптимизации. -М.: Физматлит, 2005.
[10] Васильев Ф.П. Методы оптимизации. – М.: МЦНМО, 2011.
[11] В.В.Воеводин, Вл.В.Воеводин "Параллельные вычисления", БХВ-Петербург, 2002, 608 стр.
[12] О.А.Логачев. Криптографические свойства булевых функций. Пособие. М: МАКС Пресс, 2007, С. 112.
[13] О.А.Логачев, А.А.Сальников, С.В.Смышляев, В.В.Ященко. Булевы функции в теории кодирования и криптологии. М: ЛЕНАНД, 2015, С. 576.
[14] Ю.В.Таранников. Комбинаторные свойства дискретных структур и их приложения к криптологии. М: МЦНМО, 2011, С. 152.
[15] Preneel B. Analysis and Design of Cryptographic Hash Functions, PhD Thesis, 2003.https://www.esat.kuleuven.be/cosic/publications/thesis-2.pdf (§§ 2.2.2, 2.4.1, 2.4.2, 2.5.2.1, 2.5.2.4, 2.5.2.5).
[16] Biham E., Dunkelman O. A Framework for Iterative Hash Functions – HAIFA, Cryptology ePrint Archive, 2007, https://eprint.iacr.org/2007/278 (§3).
[17] Preneel, B., Govaerts, R., Vandewalle, J. Hash functions based on block ciphers: a synthetic approach. Advances in Cryptology — CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science, vol 773, 1994, https://link.springer.com/content/pdf/10.1007/3-540-48329-2_31.pdf.
[18] Boneh D., Shoup V. A Graduate Course in Applied Cryptography, 2020, https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf (§§ 6.1, 6.3, 6.4.3, 6.5.1.2, 8.7.1, 8.7.2, 8.8.1, 8.9).
[19] Кузюрин Н. Н., Фомин С. А. Эффективные алгоритмы и сложность вычислений. Учебное пособие, МФТИ, 2007, 312 с.
[20] Arora S., Barak B., Computational Complexity: A Modern Approach. Princeton University, 2009, 594 с.
[21] Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. МЦНМО, 1999, 192 с.
[22] Применко Э. А. Алгебраические основы криптографии: учебное пособие / Э. А. Применко, Москва: МАКС Пресс, 2007. 250 с.