

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

Утвърдил:

(проф. дмн П. Бойваленков, Директор на ИМИ-БАН)

КОНСПЕКТ

за кандидат-докторантски изпит

по докторска програма Методи за обработка и защита на данни,
в сила от 2025 година

1. Собствени стойности. Собствени вектори. Спектрални теореми.
2. Кодове, поправящи грешки. Разстояние по Хеминг. Декодиране. Двоичен симетричен канал. Минимално кодово разстояние. Откриващи и декодиращи способности на кодовете.
3. Основна задача на теорията на кодирането. Граница на Хеминг и следствия. Съвършени кодове – дефиниция и примери.
4. Крайни полета, векторни пространства над крайни полета. Ортогоналност в линейни пространства над крайни полета. Линейни кодове. Дуалност.
5. Комбинаторни дизайни и структури на инцидентност – определения, примери и свойства. Симетрични дизайни.
6. Крайни геометрии и дизайни. Теореми на Брук-Райзер и Брук-Човла-Райзер.
7. Матрици на Адамар. Приложения.
8. Булеви функции. Векторни булеви функции.
9. Графи – основни понятия, представяне, видове графи.
10. Канонична форма. Изоморфизъм на графи.
11. Спектрална теория на графите.
12. Криптографска система, място и роля на криптографските методи и средства. Класически и съвременен криптоанализ.
13. Симетрична и асиметрична криптография. Блокови шифри (DES, AES).
14. Системи с публичен ключ (RSA). Електронен подпис (ЕлГамал).
15. Блокчейн – основни понятия, структура, употреба, механизми за консенсус.
16. Линейно и изпъкнало оптимиране.
17. Ефективна паралелизация на алгоритми. Основни практики. Примери в изчислителна линейна алгебра. Примери в теория на графите.

Примерна литература

1. Spectra of graphs, Brouwer A., Haemers W., <https://aeb.win.tue.nl/2WF02/spectra.pdf>, 2011
18. Fundamentals of Error-Correcting codes, W. C. Huffman, V. Pless, Cambridge University Press, 2003
19. The Theory of Error-Correcting codes, J. MacWilliams, N. J. A. Sloane, North-Holland, 1977
20. Cryptography and data security, D. E. Denning, Addison-Wesley Publishing Company, 1982
21. Coding theory and Cryptography, the essentials, D.C. Hankerson, CRC Press, 2000
22. Finite Fields, Lidl R., Niederreiter H., Cambridge University Press 1996
23. Discrete Mathematics Elementary and Beyond, Springer Undergraduate Texts in Mathematics, Lovász L., Pelikán J., Vesztergombi K., 2003
24. Analysis of Boolean Functions, O'Donnell R., May 2021 arXiv edition, <https://www.cs.cmu.edu/~odonnell/papers/Analysis-of-Boolean-Functions-by-Ryan-ODonnell.pdf>
25. В. Тончев, Комбинаторни структури и кодове, Университетско издание “Климент Охридски”, София, 1988

дата: 25.02.2024 г. Съставили:
(проф. Христо Костадинов) (гл. ас. д-р Константин Делчев)

Конспектът е обсъден и одобрен на заседания на секция „**Математически основи на информатиката**“ на 25.02.2025 г.

Ръководител секция:
(проф. Христо Костадинов)

Разгледан от Директорския съвет на ИМИ-БАН на 21.03.2025 г. (Протокол № 13).

Приет от Научния съвет на ИМИ-БАН на 28.03.2025 г. (Протокол № ...)