ЦЕНТЪР ПО ИНФОРМАТИКА И ТЕХНИЧЕСКИ НАУКИ

УЧЕБНА ПРОГРАМА

Утвърждавам:
Декан:

EN 411

КОДИРАНЕ И ЗАЩИТА НА ИНФОРМАЦИЯТА

Актуализирана: Прот.№ 23 от 28.06.2022 г.

Лектор: доц. д-р Е. Николова

АНОТАЦИЯ

Дисциплината “Кодиране и защита на информацията” е основен курс за специалностите от направления 5.3. Комуникационна и компютърна техника. Курсът формира теоретични знания за основните понятия на теория на кодирането – кодове, коригиращи грешки, разстояние на Хеминг, параметри на кодове, еквивалентност на кодове, кодиране и декодиране с линейни кодове, синдромно декодиране, основите на теорията на цикличните кодове, както и практически умения за оценяване на качествата на кодове за компресия, за оценяване на шумозащитните качества на кодове, за конструиране на кодове със зададени свойства.

ОСНОВНИ ЦЕЛИ

В курса се акцентира върху основите на оптималното кодиране, елементарни понятия от теория на информацията, основите на шумозащитното кодиране, основни класове шумозащитни кодове, някои фундаментални граници за кодове.

ПРЕДПОСТАВКИ

За успешно усвояване на материала, предвиден в курса по Кодиране и защита на информацията са необходими базови познания по дискретна математика, елементарни познания по линейна алгебра, висша алгебра, теория на вероятностите.

СТАТУТ И СТРУКТУРА

специалност	статут	Кредити	редовно обучение				задочно обучение			
			л	с	у	общ	л	с	у	общ
КСТ	Задължителна	6	30	30		60	20	10		30
СИ	Избираема	6	30	30		60	20	10		30

СЪДЪРЖАНИЕ НА КУРСА

Тема 1. Математически модел на комуникационна система. Двоичен симетричен канал без памет. Двоичен симетричен канал с изтриване. Дискретен канал с памет. Непрекъснати канали.

Тема 2. Побуквено кодиране. Префиксни кодове. Алгоритъм на Фано-Шенон. Метод на Хафман. Програмна реализация на кодове на Хафман.

Тема 3. Кодове, поправящи грешки. Основни понятия. Подходи за откриване и отстраняване на грешки. Тегло и разстояние на Хеминг. Основни принципи на декодирането.

Тема 4. Схеми за откриване на грешка. ISBN и ISSN кодове. UPC и EAN кодове.

Тема 5. Основна задача на теорията на кодирането. Граници на Сингълтън, Грийсмър и Хеминг. Еквивалентни кодове.

Тема 6. Крайни полета. Векторни пространства над крайни полета. Линейни кодове. Пораждаща матрица. Кодиране и декодиране с линейни кодове.

Тема 7. Дуален код, проверочна матрица. Синдромно декодиране.

Тема 8. Циклични кодове. Пръстен на полиномите по модул даден полином. Пораждащ полином и пораждаща матрица на цикличен код. Проверочен полином и проверочна матрица на цикличен код. Кодиране и декодиране с циклични кодове.

Тема 9. Фамилии кодове. Кодове на Хафмън. Кодове на Рид-Малер. Кодове на Рид-Соломон. БЧХ-кодове.

Тема 10. Конволюционните кодове. Структура. Кодиране с конвулюционни кодове. Декодиращ алгоритъм на Витерби.

Тема 11. Криптография - основни понятия и класически шифри.

СЕМИНАРНИ УПРАЖНЕНИЯ

Тема 1. Побуквено кодиране. Алгоритъм на Фано-Шенон. Метод на Хафмън. Програмна реализация на кодове на Хафмън.

Тема 2. Компресиращи алгоритми.

Тема 3. Линейни кодове. Основни параметри на линеен код. Пораждаща матрица в стандартна форма. Кодиране с линейни кодове.

Тема 4. Декодиране с линейни кодове. Метод на Слепян. Дуален код, проверочна матрица. Синдромно декодиране.

Тема 5. Циклични кодове. Пръстен на полиномите по модул даден полином. Пораждащ полином и пораждаща матрица на цикличен код. Проверочен полином и проверочна матрица на цикличен код.

Тема 6. Кодиране и декодиране с циклични кодове.

Тема 7. Кодиране и декодиране с конволюционни кодове.

ПЛАНИРАНИ УЧЕБНИ ДЕЙНОСТИ И МЕТОДИ НА ОБУЧЕНИЕ

1. Първата лекция има за цел студентите да се запознаят със съдържанието на програмата, целите и задачите на дисциплината, както и за изискванията за подготовка на дисциплината.
2. Лекциите са по въпроси от конспекта. Всяка от темите завършва с въпроси и задачи за самоподготовка.
3. Студентите работят по индивидуални задания по време на семинарните занятия, които формират текущ контрол.
4. Текущият контрол се реализира и чрез курсовата работа, както и чрез контролни работи.
5. Електронните материали в платформа Moodle подпомагат подготовката на студентите и предоставят възможности за разширяване на познанията им по някои от темите.

Теоретичният материал е представен с помощта на следните ресурси:

- Книги – съдържат теоретичен материал по темите;
- Страници - съдържат кратък теоретичен материал или допълнителни пояснения;
- Web ресурси - статии, онлайн списания, готови шаблони и други материали;
- Видеоматериали - включват видеоуроци;
- Файлове.

Практическата работа е реализирана чрез следните ресурси и дейности:

- Задания – студентите решават самостоятелно поставени от преподавателя задачи, като решенията се оценяват от преподавателя;
- Тестове – за самоподготовка и самопроверка на усвоените знания;
- Web ресурси – статии, онлайн списания, готови шаблони и други материали;
- Видеоматериали - включват видеоуроци за създаването на конкретни модели;
- Форум – използва се за консултиране на студентите от преподавателите и обмен на информация между студентите;
- Видеоконферентна връзка – използва се за периодични консултации в реално време между студентите и преподавателите.

МЕТОДИ ЗА ОЦЕНЯВАНЕ

През семестъра се извършва текущ контрол на придобитите знания, като резултатите се оформят по точкова система. Текущият контрол се реализира чрез две контролни работи. Курсовата задача се приема и оценява от ръководителя на упражненията. До изпит се допускат студентите, предали и защитили и двата модула. Изпитът се провежда писмено в две части – задачи и теория. До теоретичната част на изпита се допускат само студентите с положителна оценка на задачи. Крайната оценка е комплексна и включва оценките от текущия контрол, курсовата задача и оценката от изпита. Сумарният брой точки определя размера на крайната шестобална оценка по схемата:

1. Оценка от текущ контрол до 34 точки
2. Оценка от курсовата работа до 12 точки
3. Оценка от семестриалния изпит до 54 точки

Общата оценка се определя от сумата на точките през семестъра и от изпитната процедура: 36-50т. – Среден (3); 51-65 т. – Добър (4); 66-80 т.–Мн. Добър(5); Над 81 т.–Отличен (6).

Студентът трябва да има минимум 14 точки от контрола през семестъра и минимум 22 точки от изпитната процедура, за да му се формира комплексна оценка.

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА

1. Е. Великова-Бандова, Записки по кодиране - Двоични шумозащитни кодове, ФОИ-КОМЕРСЕ, София, 2001.
2. Е. Великова-Бандова, Записки по кодиране - Циклични кодове, ФОИ-КОМЕРСЕ, София, 2001.
3. Raymond Hill. A first course in Coding Theory. University of Salford. Clarendon Press. Oxford, 2012.
4. J.H. van Lint, Introduction to Coding Theory, Springer Verlag, Berlin, 2021.
5. V. Pless, Introduction to the Theory of Error-Correcting Codes, John Wiley, New York, 2015.

6. D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, Coding theory. The essentials, Marcel Dekker INK, New York, 1992, http://index-of.co.uk/Information-Theory/Coding%20Theory%20The%20Essentials%20-%20D.G%20Hoffman.pdf
7. R. W. Yeung, Shuo-Yen Robert Li, Ning Cai, Zhen Zhang, Network coding theory, now Publishers Inc., Hanover, 2006, http://iest2.ie.cuhk.edu.hk/~whyeung/publications/tutorial.pdf

ИЗПИТЕН ВЪПРОСНИК

EN 411

КОДИРАНЕ И ЗАЩИТА НА ИНФОРМАЦИЯТА

Лектор: доц. д-р Е. Николова

Тема 1. Математически модел на комуникационна система. Двоичен симетричен канал без памет. Двоичен симетричен канал с изтриване. Дискретен канал с памет.

Тема 2. Побуквено кодиране. Префиксни кодове. Алгоритъм на Фано-Шенон.

Тема 3. Метод на Хафман. Програмна реализация на кодове на Хафман.

Тема 4. Подходи за откриване и отстраняване на грешки.

Тема 5. Основни принципи на декодирането.

Тема 6. Схеми за откриване на грешка. ISBN и ISSN кодове. UPC и EAN кодове.

Тема 7. Основна задача на теорията на кодирането. Граници на Сингълтън, Грийсмър и Хеминг.

Тема 8. Крайни полета. Векторни пространства над крайни полета.

Тема 9. Линейни кодове. Пораждаща матрица. Еквивалентни линейни кодове.

Тема 10. Кодиране и декодиране с линейни кодове.

Тема 11. Дуален код, проверочна матрица. Синдромно декодиране.

Тема 12. Циклични кодове. Пръстен на полиномите по модул даден полином. Пораждащ полином и пораждаща матрица на цикличен код. Проверочен полином и проверочна матрица на цикличен код.

Тема 13. Кодиране и декодиране с циклични кодове.

Тема 14. Кодове на Хафмън.

Тема 15. Кодове на Рид-Малер.

Тема 16. Кодове на Рид-Соломон.

Тема 17. БЧХ-кодове.

Тема 18. Конволюционните кодове. Структура. Кодиране с конвулюционни кодове.

Тема 19. Декодиращ алгоритъм на Витерби.

Тема 20. Криптография - основни понятия и класически шифри.

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА

8. Е. Великова-Бандова, Записки по кодиране - Двоични шумозащитни кодове, ФОИ-КОМЕРСЕ, София, 2001.
9. Е. Великова-Бандова, Записки по кодиране - Циклични кодове, ФОИ-КОМЕРСЕ, София, 2001.
10. Raymond Hill. A first course in Coding Theory. University of Salford. Clarendon Press. Oxford, 2012.
11. J.H. van Lint, Introduction to Coding Theory, Springer Verlag, Berlin, 2011.
12. V. Pless, Introduction to the Theory of Error-Correcting Codes, John Wiley, New York, 2015.

13. D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall, Coding theory. The essentials, Marcel Dekker INK, New York, 1992, http://index-of.co.uk/Information-Theory/Coding%20Theory%20The%20Essentials%20-%20D.G%20Hoffman.pdf
14. R. W. Yeung, Shuo-Yen Robert Li, Ning Cai, Zhen Zhang, Network coding theory, now Publishers Inc., Hanover, 2006, http://iest2.ie.cuhk.edu.hk/~whyeung/publications/tutorial.pdf