помогою конструювання його графів-циклів. Граф-цикл, відомий також як просто n-цикл, представляє собою граф, що містить n вузлів і складається з єдиного циклу, що проходить через всі його вузли. Число вершин у графі-циклі дорівнює числу ребер, кожна вершина має ступінь 2 – будь-яка вершина інцидентна рівно двом ребрам. Для візуального відображення структури графа станів ЛКГ використано орієнтований граф-цикл, у якому всі дуги спрямовані в одному і тому ж напрямку. Наведено приклади таких графів для деяких параметрів ЛКГ. Узагальнено проаналізовані структури та представлено типові графи для ЛКГ. Визначено параметри ЛКГ, характерні для його типових графів. Отримані результати дозволять більш ефективно визначати параметри ЛКГ з урахуванням можливості застосування методу формування рівномірно розподілених псевдовипадкових чисел шляхом конкатенації циклів і предциклів генератора.

31. ДОСЛІДЖЕННЯ ЗДАТНОСТІ ВИЯВЛЕННЯ ПОМИЛОК ФАКТОРІАЛЬНИМ КОДОМ З ДЕКІЛЬКОМА КОНТРОЛЬНИМИ СУМАМИ

к.т.н, доцент Фауре Е.В., магістрант Бойко А.Ю., ЧДТУ, Черкаси

У роботі розглянуто методи факторіального кодування з декількома контрольними сумами, що комплексно вирішують задачі контролю цілісності інформації та її криптографічного захисту та спрямовані на скорочення часу формування кодового слова і обсяг використовуваної для цього пам'яті. Метод роздільного факторіального кодування з декількома контрольними сумами використовує в якості перевірної частини кодового слова конкатенацію декількох перевірних частин, обчислених за окремими частинами інформаційного блоку. Нероздільне кодування з декількома контрольними сумами передбачає заміну інформаційної послідовності на конкатенацію декількох перестановок, обчислених за різними частинами інформаційної послідовності. Для запропонованих методів кодування вивчені залежності оцінок ймовірності невиявленої помилки й енергетичного виграшу від довжини інформаційного вектора на вході кодера. Проведено порівняння показників виявляючої здатності для факторіальних кодів з декількома контрольними сумами та інших завадостійких кодів

32. ДОСЛІДЖЕННЯ ЗДАТНОСТІ ВИЯВЛЕННЯ ПОМИЛОК ФАКТОРІАЛЬНИМ КОДОМ З ВІДНОВЛЕННЯМ ДАНИХ

к.т.н, доцент Фауре Е.В., магістрант Юрченко В.Л., ЧДТУ, Черкаси

У доповіді розглянуто особливості забезпечення захисту інформації за допомогою факторіального кодування з відновленням даних (ФКВД). ФКВД дозволяє забезпечити: захист від несанкціонованого читання інформації; виявлення помилок, що вносяться каналом зв'язку в процесі передавання повідомлення приймачу; властивість самосинхронізації (можливість циклової синхронізації системи – знаходження меж блоків). Кодове слово ФКВД представляє собою перестановку, що обчислюється за всіма бітами інформаційного вектора. У процесі роботи досліджено аналіз залежності енергетичного виграшу в результаті застосування ФКВД від довжини інформаційної частини кодового слова, а також проведена верифікація математичної моделі для виявляючої здатності ФКВД за допомогою імітаційного моделювання. Сформульовано рекомендації щодо застосування ФКВД для задач захисту інформації.

33. ДОСЛІДЖЕННЯ ПРОЦЕДУРИ ФОРМУВАННЯ КОНТРОЛЬНОЇ СУМИ ПОВНОГО ФАКТОРІАЛЬНОГО КОДУ НА ОСНОВІ ЗАЛИШКУ ЗА МОДУЛЕМ

к.т.н, доцент Фауре Е.В., аспірант Харін О.О., Литвиненко Д.О., ЧДТУ, Черкаси

У доповіді розглянуто особливості формування контрольної суми для повного факторіального коду (ПФК). Контрольна сума ПФК представляє собою перестановку, що обчислюється за всіма бітами інформаційного вектора. У роботі досліджено процедуру формування синдрому перестановки на основі залишку за модулем. Для цього

розроблено програмну модель, що дозволяє дослідити вплив помилок, які виникають у каналі зв'язку, на значення контрольної суми, що обчислюється в декодері. За допомогою розробленої моделі накопичено статистику для визначення розподілу значень контрольної суми в залежності від ваги помилки, розміру інформаційної і перевірної частин, а також ключів формування перестановки. Аналіз отриманих результатів дозволив визначити ймовірність невиявленої помилки під час передавання кодового слова ПФК каналом зв'язку з незалежними помилками, а також у випадку несанкціонованої модифікації переданих даних.

34. ДОСЛІДЖЕННЯ ПРОЦЕДУРИ ФОРМУВАННЯ КОНТРОЛЬНОЇ СУМИ ПОВНОГО ФАКТОРІАЛЬНОГО КОДУ НА ОСНОВІ ІТЕРАЦІЙНОГО ПЕРЕТВОРЕННЯ

к.т.н, доцент Фауре Е.В., аспірант Харін О.О., Качалова М.О., ЧДТУ, Черкаси

У доповіді розглянуто особливості формування контрольної суми для повного факторіального коду (ПФК). Контрольна сума ПФК представляє собою перестановку, що обчислюється за всіма бітами інформаційного вектора. У роботі досліджено процедуру формування синдрому перестановки на основі ітераційного перетворення. Для цього запропоновано розрахунково-експериментальну модель, що дозволяє дослідити вплив помилок, які виникають у каналі зв'язку, на значення контрольної суми, що обчислюється в декодері. За допомогою розробленої моделі накопичено статистику для визначення розподілу значень контрольної суми в залежності від ваги помилки, розміру інформаційної і перевірної частин, а також ключів формування перестановки. Аналіз отриманих результатів дозволив визначити ймовірність невиявленої помилки під час передавання кодового слова ПФК каналом зв'язку з незалежними помилками, а також у випадку несанкціонованої модифікації переданих даних.

35. TO THE PROBLEMS OF THE TEXTUAL INFORMATION PROCESSING AUTOMATION IN MODERN COMPUTER SYSTEMS

Tarasenko Ya., ChSTU, Cherkassy

The report is considered with the main technical problems of the processing automation of the textual data depending on the target computer system, it was also analyzed the relevance and practical application. The main methods of textual information processing and their automation features are investigated. The ways of solving problems connected with the imperfection of computer processing of the text, written in the natural language, which are based on the creation of an algorithm that implements elements of computer hermeneutics and discursive analysis were suggested. The research has shown that the method acts as a tool that improves the automated analysis of the text and reduces the risk of inconsistencies appearance during the work with the object of analysis, caused by the ambiguity of the natural language.

36. ПРОГРАМНЕ МОДЕЛЮВАННЯ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ДЛЯ ДОСЛІДЖЕННЯ КРИПТОПРИМІТИВІВ

Стабецька Т.А., ЧДТУ, Черкаси

У доповіді представлено розроблені методи синтезу прямих та обернених операцій розширеного матричного криптографічного перетворення довільної кількості аргументів, адаптовані до їх програмної реалізації. Побудовано блок-схеми алгоритмів, які забезпечили реалізацію операцій розширеного матричного криптографічного перетворення довільної кількості аргументів. Запропоновано варіанти застосування операцій розширеного матричного криптографічного перетворення довільної кількості аргументів у криптоалгоритмах.