**Булах Євгеній Вячеславович. Кінцеві автомати з псевдовипадковими переходами і методи захисту інформації на їх основі: дис... канд. техн. наук: 05.13.13 / Харківський національний ун-т радіоелектроніки. - Х., 2004.**

|  |  |
| --- | --- |
| |  | | --- | | Булах Е.В. Кінцеві автомати з псевдовипадковими переходами і методи захисту інформації на їх основі – Рукопис.  Дисертація на здобуття вченого ступеня кандидата технічних наук за фахом 05.13.13 – обчислювальні машини, системи і мережі. – Харківський національний університет радіоелектроніки, Харків, 2004.  Дисертація присвячена розробці алгоритмів функціонування кінцевих автоматів із псевдовипадковими переходами із одного стану в інший, які є завадостійкими до віртуальних послідовностей, і здійснюють одномірний пошук точки екстремуму унімодальної функції. Такі кінцеві автомати є генераторами шифру заміни (підстановки) для символів вхідного алфавіту. Підстановки, що формуються таким автоматом, дозволили для одного й того ж самого символу генерувати множину підстановок різної довжини (генеруються префіксні коди). Вибір підстановок для того ж самого символу вхідного алфавіту здійснюється псевдовипадковим чином. Різноманіття алгоритмів функціонування кінцевих автоматів із псевдовипадковими переходами, які є завадостійкими до віртуальних послідовностей, і використання запропонованих кодів значно ускладнює процес розкриття шифротекста.  Результати роботи використано при виконанні держбюджетних НДР по створенню нових методів захисту інформації при її збереженні і передачі (д/б 190232 "Розробка теорії і методів захисту інформації при її передачі і збереженні", д\б 190 (520-7) "Система захисту інформації при її передачі в інтелектуальних середовищах"), а також використовуються в навчальному процесі при виконанні лабораторних робіт і дипломному проектуванні у Харківському національному університеті радіоелектроніки. | |
| |  | | --- | | У дисертаційній роботі приведено результати, котрі у відповідності з метою дослідження в сукупності вирішують актуальну наукову задачу – створення нових методів захисту інформації на базі розроблених методів логічного синтезу кінцевих автоматів із псевдовипадковими переходами з одного стану в інше. Такі кінцеві автомати можуть бути застосовані у аналого-цифрових перетворювачах, при завадостійкому пошуку даних, при завадостійкому пошуку несправного елемента, при завадостійких запитальниках, в теорії кодування при пошуку точки екстремуму унімодальної функцій.  Основні наукові і практичні результати дисертаційної роботи такі.  1. Проаналізовано існуючи методи захисту інформації, та виявлено, що одним з рішень задач збільшення невизначеності є використання нерівнозначного кодування. Для реалізації цього принципу запропоновано застосування датчиків віртуальних послідовностей і завадостійких до них алгоритмів пошуку точки екстремуму унімодальної функції.  2. Створено алгоритмічні основи синтезу КА з псевдовипадковими переходами на базі завадостійких до регулярних несиметричних і симетричних віртуальних послідовностей алгоритмів одномірного пошуку точки екстремуму унімодальної функції. Одержано співвідношення для розв'язуючої функції (правила виділення нового інтервалу невизначеності) і стратегії пошуку (розподіл точок експерименту в ізнов виділеному інтервалі невизначеності) завадостійких алгоритмів пошуку точки екстремуму унімодальної функції та схеми їх побудови. Це дало змогу організувати псевдовипадковий вибір підстановок символів вхідного алфавіту, які являють собою нерівнозначні префіксні коди [7].  3. Створено алгоритмічні основи синтезу КА з псевдовипадковими переходами на базі завадостійких до нерегулярних (тривалість збурювання є випадкова величина) несиметричних і симетричних віртуальних послідовностей алгоритмів одномірного пошуку точки екстремуму унімодальної функції. Одержано співвідношення для розв'язуючої функції і стратегії пошуку завадостійких до несиметричних і симетричних нерегулярних віртуальних послідовностей алгоритмів пошуку точки екстремуму унімодальної функції, що описують функціонування кінцевих автоматів із псевдовипадковими переходами, і які є генераторами псевдовипадкових підстановок символів вхідного алфавіту [3, 6].  4. Розроблено методи побудови надлишкових уявлень десятинних чисел на основі отриманих числових рядів. Ці методи характеризуються тим, що для одного і того ж символу вхідного алфавіту існує множина підстановок різної довжини, а їх вибір здійснюється псевдовипадковим чином. Здобуто оцінки ефективності алгоритмів пошуку у вигляді рядів цілих позитивних чисел дозволили створити надлишкові уявлення чисел і сумістити захист інформації від дії завад у каналі та від несанкціонованого доступу [4, 6].  5. Розроблено структурні схеми нових датчиків віртуальних послідовностей для організації псевдовипадкових переходів КА. Створено структурні схеми КА, кодуючих і декодуючих пристроїв для каналу передачі інформації на основі завадостійких до віртуальних послідовностей алгоритмів пошуку [1], [2].  6. Проведено оцінку ступеня захищеності інформації при її передачі. При цьому ураховувалися алгоритм функціонування КА, конкретна унімодальна функція однієї змінної, тип віртуальної послідовності та її параметри. Показано, що якщо по дискретному каналі передається 64 цифри восьмеричної системи, то невизначеність (кількість варіантів перебору) складе [5].  7. Розроблено пристрій керування вихідними потужними електронними ключами за рахунок псевдовипадкових імпульсів з заданими параметрами на основі завадостійких алгоритмів, що отримані у дисертаційній роботі. Використання таких пристроїв у автономних джерелах електрозабезпечення газорозподільних станцій, які розроблено у НПФ „Газінжінірінг-сервіс”, дозволяє уникнути імпульсних низькочастотних навантажень на електрогенератор. | |