Національна академія наук України
Інститут кібернетики імені В. М. Глушкова

На правах рукопису

ПОНОМАРЬОВ Аскольд Анатолійович

МАТЕМАТИЧНІ МЕТОДИ І ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ЗОВНІШНІХ ЗАПАМ'ЯТОВУЮЧИХ ПРИСТРОЇВ

01.05.03 — математичне та програмне забезпечення обчислювальних машин і систем

Автореферат дисертації на здобуття наукового ступеня кандидата фізико-математичних наук

Київ 1997

Дисертацією є рукопис.

Робота виконана в Інституті кібернетики ім. В. М. Глушкова та Науково-учбовому центрі прикладної інформатики Національної академії наук України.

Наукові керівники: член-кореспондент Академії інженерних наук України, доктор технічних наук БАРДАЧЕНКО Віталій Феодосійович,

доктор фізико-математичних наук, професор ГУПАЛ Анатолій Михайлович.

Офіційні опоненти: доктор фізико-математичних наук, професор КНОПОВ Павло Соломонович,

кандидат фізико-математичних наук ДОМРАЧЕВ Володимир Миколайович.

Провідна організація: Київський національний університет ім. Т. Г. Шевченка.

Захист відбудеться «23» травня 1997 р. о 11 год. на засіданні спеціалізованої вченої ради Д 01.39.02 при Інституті кібернетики ім. В. М. Глушкова НАН України за адресою:

252022 Київ 22, проспект Академіка Глушкова, 40.

З дисертацією можна ознайомитися в науково-технічному архіві інституту.

Автореферат розіслано «11» квітня 1997 року.

Учений секретар спеціалізованої вченої ради СИНЯВСЬКИЙ В. Ф.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність роботи. В умовах становлення України як суверенної держави, коли відбувається формування багатоукладної економіки на фоні широкого впровадження передових інформаційних технологій, питання безпеки інформації набувають найвищого пріоритету у всій сфері національної безпеки. Зважаючи на особливу громадську небезпеку комп'ютерних злочинів, що завдають значної шкоди державним і комерційним структурам, проблема технічного захисту інформації у засобах обчислювальної техніки, автоматизованих комп'ютерних системах та мережах ЕОМ є вельми важливою.

Державною службою України з питань технічного захисту інформації (тепер - Державний комітет України з питань державних секретів і технічного захисту інформації) окреслені пріоритетні напрями розвитку системи технічного захисту інформації в галузі інформатизації, створення наукової і матеріально-технічної бази системи комп'ютерної безпеки, що являє собою частину загальнодержавної системи безпеки інформації. Деякі напрями безпосередньо стосуються математичних методів і технічних засобів захисту інформації зовнішньої пам'яті ЕОМ.

Оскільки зберігання - найбільш критична з точки зору уразливості стадія обробки даних в автоматизованих системах, саме зовнішня пам'ять, що представлена широким класом електромеханічних зовнішніх запам'ятовуючих пристроїв (ЗЗП), відіграє ключову роль у розв'язанні задачі захисту інформації від загроз безпеці різноманітного характеру. Серед можливих розв'язків, що називаються вказаною службою, - розробка перспективних засобів і методів кодування, запису, обробки і передачі інформації, створення технологій і засобів довгострокового безпечного зберігання даних в обчислювальних системах.

Особливої уваги заслуговує питання криптографічного захисту інформації ЗЗП, тим більш, що воно тісно пов'язане з проблемою створення в Україні вітчизняних криптографічних систем, методів і технічних засобів, від якості яких залежить безпека багатьох юридичних і фізичних осіб, а в ряді випадків і всієї держави.

Таким чином, дисертаційна робота, в якій пропонуються принципово нові підходи до технічного захисту інформації ЗЗП, уявляється актуальною і своєчасною.

Метою роботи є створення математичних методів і технічних засобів захисту інформації ЗЗП, направлених на розв'язання проблем

криптографічно якісних генераторів псевдовипадкових чисел (ПВЧ) і високоефективних кодів з обмеженими довжинами серій.

Задачі дослідження. Поставлена мета визначає наступні задачі.

1. Проведення всебічного аналізу відомих математичних методів і технічних засобів захисту інформації ЗЗП.

2. Розробка криптографічно якісних алгоритмів вироблення ПВЧ.

3. Дослідження на ЕОМ криптографічних властивостей створених алгоритмів за допомогою спеціальної системи емпіричних тестів.

4. Розробка програмних і апаратних засобів потокового шифрування інформації ЗЗП з використанням нових генераторів ПВЧ.

5. Створення методів побудови високоефективних кодів з обмеженими довжинами серій.

6. Оцінка завадозахищеності інформації у випадку застосування нового кодування.

7. Розробка способів цифрового магнітного запису (ЦМЗ) на базі побудованих високоефективних канальних кодів.

8. Створення основ технічної реалізації нових канальних кодів і способів ЦМЗ.

Методи дослідження. У роботі використані методи теорії детермінованого хаосу, теорії імовірностей і математичної статистики, теорії таймерних обчислювальних систем, теорії кодування, методи математичного моделювання.

Наукова новизна. В роботі вперше отримані наступні наукові результати.

1. На основі аналізу математичних методів і технічних засобів захисту інформації ЗЗП виконано формалізацію проблеми технічного захисту інформації зовнішньої пам'яті у вигляді інформаційної моделі ЗЗП і визначено напрями дослідження.

2. Запропоновано і науково обґрунтовано використання в криптографічних цілях теорії детермінованого хаосу, що базується на концепції дивного аттрактора.

3. Розроблено і програмно реалізовано систему емпіричних тестів, яка дозволяє скласти комплексну оцінку властивостей генератора ПВЧ, орієнтованого на застосування в криптографічному захисті інформації. Показано неспроможність відомих алгоритмів вироблення ПВЧ у розв'язанні задач криптографії.

4. За допомогою обчислювальних експериментів з відомими математичними моделями Лоренца і Хенона доведено принципову можливість побудови криптографічно якісних джерел випадкових і псевдовипадкових числових послідовностей на основі дивних аттракторів.

5. Побудовано і досліджено нову, цілочисельну математичну модель динамічної системи з дивним аттрактором. На її основі розроблено генератор ПВЧ, що в повній мірі відповідає всім вимогам, які ставляться до криптографічно якісних алгоритмів.

6. Запропоновано використання в системах ЦМЗ принципів подання інформації в таймерному вигляді і її обробки за допомогою таймерних обчислювальних пристроїв. Показано, що таймерне розрядно-аналогове кодування в поєднанні з перетворенням в системах числення з невеликою основою забезпечує підвищення завадозахищеності інформації ЗЗП.

7. Розроблено метод побудови кодів з обмеженими довжинами серій на основі таймерного розрядного представлення інформації, застосування якого дозволяє значно покращити технічні характеристики ЗЗП.

8. Запропоновано винахід нових способів ЦМЗ, які розв'язують задачу підвищення щільності запису за рахунок поєднання таймерних принципів представлення інформації з перекодуванням в системах числення з основою більше двох.

9. Створено метод таймерного трійкового кодування (ТТК), який забезпечує значне підвищення рівня некриптографічного захисту інформації в системах цифрового запису і зв'язку, в тому числі збільшення щільності запису, швидкості передачі, завадозахищеності, надійності функціонування.

10. Розроблено основи технічної (програмної і апаратної) реалізації нових математичних методів захисту інформації ЗЗП.

Достовірність дослідження підтверджена результатами багаточисельних обчислювальних експериментів над математичними моделями на ЕОМ і даними практичних експериментів над розробленими дослідними зразками технічних засобів (програмних і апаратних), що повністю відповідають теоретичним висновкам.

Практична цінність та впровадження. Створені математичні методи захисту інформації ЗЗП і розроблені основи їх реалізації у вигляді технічних засобів дозволяють забезпечити високий рівень конфіденційності, цілісності, доступності і надійності даних при їх обробці, зберіганні і передачі. Генератор ПВЧ на основі цілочисельного дивного аттрактора, таймерне трійкове кодування і спосіб ЦМЗ на його основі - головні наукові результати, які мають безпосередню практичну направленість. Області їх можливого застосування - відповідальні системи потокового шифрування, системи ЦМЗ і цифрового зв'язку, захищені засоби обчислювальної техніки.

Частина практичних результатів отримана автором за участю в двох науково-дослідних роботах (1994-1995) і відображена у відповідних заключних звітах.

Наукові результати роботи використані при створенні проекту міждержавного стандарту "Засоби обчислювальної техніки. Системи мікропроцесорні таймерні. Загальні технічні вимоги", що схвалений національними органами по стандартизації України, Російської Федерації, Республіки Білорусь, Республіки Молдова; на Київському науково-виробничому об'єднанні "Електронмаш" при виготовленні дослідних зразків таймерного телефонного маскіратора "Криптел"; там же при виготовленні дослідних зразків замка з електронним ідентифікатором особи, який кодується вручну, та при розробці технічно-конструкторської документації для початку його серійного виробництва.

Апробація роботи. Основні результати роботи доповідались

на VII Українській конференції "Моделювання і дослідження стійкості систем" (Київ, 1996);

на науково-практичній конференції "Програмно-технічні засоби інформатизації освіти" (Київ, 1995);

на семінарах "Математичне моделювання в наукових дослідженнях" і "Таймерні обчислювальні пристрої" наукової ради НАН України з проблеми "Кібернетика" (Київ, 1994-1996);

в Інституті кібернетики ім. В.М.Глушкова НАН України на науковому семінарі за матеріалами дисертації (1997).

Наукові результати роботи в області таймерного кодування інформації згадуються в річних (1994, 1996) звітах НАН України.

За результатами наукових досліджень автору на конкурсній основі присуджувались стипендія НАН України для молодих учених (1994-1997) і грант Міжнародної асоціації академій наук і НАН України для молодих учених (1996).

Публікації. За темою дисертації опубліковано 12 друкованих робіт, отримано патент Російської Федерації.

Структура і обсяг роботи. Дисертація складається із вступу, чотирьох глав, висновків, переліку літератури (250 найменувань), додатків і містить 135 сторінок машинописного тексту (включаючи 9 таблиць) та 20 рисунків.

ЗМІСТ РОБОТИ

Вступ містить обґрунтування актуальності проблеми інформаційної безпеки і, зокрема, технічного захисту інформації ЗЗП.

У першій главі "Аналіз математичних методів і технічних засо-

бів захисту інформації ЗЗП" проведено всебічний аналіз відомих математичних методів і технічних засобів захисту інформації ЗЗП, здійснено формалізацію проблеми і визначено напрями дослідження.

Докладно розглянуто такі питання: проблеми захисту інформації в автоматизованих системах; зовнішні запам'ятовуючі пристрої надійність зберігання даних; криптографічні системи, методи і засоби захисту інформації; методи кодування і реєстрації даних. Проведений аналіз дозволив формалізувати проблему технічного захисту інформації зовнішньої пам'яті у вигляді інформаційної моделі ЗЗП.

Ця модель включає замкнений цикл передачі даних, який містить чотири фази оборотного перетворення інформації (рис.1). При тому, що кожна фаза окремо вносить свій певний вклад в загальний рівень інформаційної безпеки, разом всі фази забезпечують конфіденційність, цілісність, доступність і надійність інформації ЗЗП.

Рис. 1. Інформаційна модель ЗЗП

Тоді як методи компресійного та коректуючого кодування достатньо добре розроблені і в теоретичному, і в прикладному аспектах, криптографічні методи та способи цифрового запису інформації вимагають значного удосконалення. Тим більш, що саме фази криптографічного перетворення і канального кодування є визначальними у забезпеченні захисту інформації ЗЗП. У цьому плані особливої уваги заслуговують проблеми криптографічно якісних генераторів ПВЧ і високоефективних кодів з обмеженими довжинами серій.

У другій главі "Розробка криптографічних методів з використанням дивних аттракторів" запропоновано підхід до побудови ефективних систем потокового шифрування, який базується на концепції дивного аттрактора; на його основі розроблено криптографічно якісні генератори ПВЧ, їх властивості досліджено за допомогою створеної системи емпіричних тестів у порівнянні з відомими алгоритмами.

У системах потокового шифрування, як правило, застосовується оборотний процес накладання псевдовипадкової двійкової послідовності (гами шифру) на відкриті дані шляхом логічної операції "виключне АБО", внаслідок чого відбувається повне нівелювання частот двійкових символів і приховування смислу інформації, що захищається. При цьому джерелом гами шифру служить алгоритм вироблення (генератор) ПВЧ, що керується відносно коротким ключем. З метою утруднення криптоаналізу гама шифру повинна мати високу непередбаченість, наближаючись до дійсно випадкової послідовності.

В основу запропонованого підходу до створення альтернативних алгоритмів покладено концепцію дивного аттрактора, на якій базується теорія детермінованого хаосу. Ідея полягає в тому, що саме дивний аттрактор повинен бути криптографічно якісним джерелом псевдовипадкової числової послідовності.

Аттрактором називається притягуюча множина у фазовому просторі, до якої прагнуть всі фазові траєкторії дисипативної динамічної системи. Динамічна система із дивним аттрактором є повністю детермінованою, оскільки її розв'язки визначаються початковими даними. Проте з часом ці розв'язки змінюються надзвичайно нерегулярним чином. Для зовнішнього спостерігача, що слідкує за грубими властивостями системи, картина її поведінки виглядає повністю хаотичною. Інша важлива властивість дивних аттракторів полягає в чутливості до початкових даних: малі відхилення початкових умов викликають великі відхилення у поведінці розв'язків системи через деякий проміжок часу. І хаотична поведінка, і чутливість до початкових даних визначаються фрактальною структурою дивного аттрактора.

Таким чином, концепція дивного аттрактора максимально підходить для створення криптографічно якісних генераторів ПВЧ. Повний детермінізм математичних моделей із дивними аттракторами, з одного боку, і зовнішньо хаотична їх поведінка і чутливість до початкових даних - з іншого, повинні забезпечувати надзвичайно малу завбачуваність числових послідовностей, які виробляються, поряд з високою стабільністю статистичних характеристик.

Автором розроблено і програмно реалізовано систему емпіричних тестів, яка дозволяє скласти комплексну оцінку генератора ПВЧ, що орієнтований на використання в криптографічному захисті інформації. Система включає перевірку довжини періоду псевдовипадкової послідовності; оцінку частот цифр, які видаються генератором ПВЧ, за допомогою критерію згоди хі-квадрат; виявлення тренду у вихідній числовій послідовності з використанням статистичного критерію

серій; корреляційний аналіз, зокрема, обчислення коефіцієнта послідовної корреляції; визначення лінійної складності псевдовипадкової послідовності, що формується, методом Берлекемпа - Мессі.

Аналіз двох відомих базових методів отримання ПВЧ показав їх повну неспроможність у розв'язанні задач криптографії. Лінійний конгруентний алгоритм відзначається наявністю всередині- і міжрозрядної корреляції, а генератор ПВЧ на основі лінійного регістру зсуву із зворотним зв'язком характеризується вкрай низькою лінійною складністю.

Далі в дисертаційній роботі на основі відомих математичних моделей з дивними аттракторами Лоренца і Хенона будуються генератори ПВЧ і проводиться всебічне дослідження їх властивостей.

Поведінка системи, яка описується класичною моделлю Е. Лоренца

$$\begin{cases} dx / dt = -10x + 10y, \\ dy / dt = 28x - y - x \cdot z, \\ dz / dt = -8/3\, z + x \cdot y, \end{cases} \qquad (1)$$

являє собою рух по спіралі, що поперемінно розкручується довкола двох фокусів $C\,(6\sqrt{2},\ 6\sqrt{2},\ 27)$ і $C'\,(-6\sqrt{2},\ -6\sqrt{2},\ 27)$. При цьому перехід із околу одного фокуса в окіл іншого має нерегулярний характер, і кожна початкова точка задає свою неповторну послідовність таких переходів. Символічний опис дивного аттрактора Лоренца у вигляді "нулів" і "одиниць", котрі відповідають обертам спіралі фазової траєкторії довкола фокусів, дає двійкову числову послідовність.

Аналогова реалізація моделі Лоренца дозволяє побудувати давач випадкових чисел, висока стабільність статистичних характеристик якого забезпечується внутрішнім детермінізмом закладених у його основу рівнянь, а відсутність фізичного джерела шуму приводить до підвищення швидкодії і зменшення апаратної складності пристрою.

Цифровий генератор ПВЧ на основі аттрактора Лоренца, що реалізує чисельне інтегрування системи рівнянь (1), являє собою алгоритм вироблення двійкової послідовності шляхом символічного опису аттрактора з наступною її децимацією по індексу 7. Псевдовипадкова послідовність, що формується, відзначається великим періодом, рівномірним законом розподілу, відсутністю тренда і автокорреляції, високою лінійною складністю.

Більш простою є модель М. Хенона, двовимірне відображення

$$\begin{cases} x_{i+1} = 1 + y_i - 1{,}4\, x_i^2, \\ y_{i+1} = 0{,}3\, x_i, \quad i = 0, 1, 2, \ldots \end{cases} \qquad (2)$$

із дивним аттрактором, який займає обмежену область на площині і має вигляд ряду більш або менш паралельних "кривих" (парабол).

Генератор ПВЧ на основі дивного аттрактора Хенона являє собою алгоритм вироблення двійкової послідовності шляхом символічного опису розділеного (горизонтальною прямою) на дві частини аттрактора з наступною її децимацією по індексу 7. Як і у випадку моделі Лоренца, цей алгоритм характеризується відмінними якостями.

Проте, обидва генератори ПВЧ (особливо перший) мають значно обмежену продуктивність, що пов'язано із необхідністю використання для їх реалізації математики з плаваючою точкою.

Автором побудована нова, цілочисельна математична модель динамічної системи, що має такий вигляд:

$$\begin{cases} x_{i+1} = \dfrac{2M}{3} + \dfrac{y_i}{3} - \left(\dfrac{x_i}{\lambda} - \sqrt{M} \right)^2 \bmod M, \\ y_{i+1} = x_i, \quad i = 0, 1, 2, \ldots, \end{cases} \qquad (3)$$

де λ - керуючий параметр, M - модуль, вибраний рівним 2^{32}.

Здійснені обчислювальні експерименти показали, що система (3) має дивний аттрактор, який існує в цілочисельному фазовому просторі і розвивається за класичною схемою. Конкретно: при зменшенні керуючого параметра λ в діапазоні значень від 50000 до 35000 відбувається каскад біфуркацій типу подвоєння періоду, внаслідок чого з'являється дивний аттрактор у вигляді квазіпаралельних фрактальних парабол. При цьому дана динамічна система повністю підпорядковується закону універсальності М.Фейгенбаума. В ході подальшого зменшення керуючого параметра притягуюча множина зазнає лише монотонних змін. Вони полягають у поступовому стисненні парабол аттрактора і появі нових бокових квазіпаралельних віток, що також стискаються, і більше й більше заповнюють фазовий простір (рис.2).

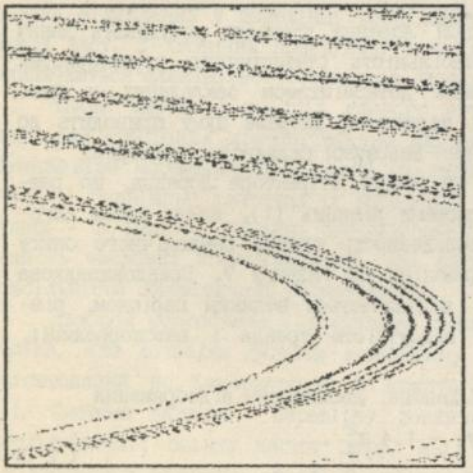

Рис.2. Цілочисельний дивний аттрактор при $\lambda = 20000$

Коли величина λ досягає свого найменшого значення 1, відбувається "схлопування" парабол з одночасним "розмиванням" дивного аттрактора по усьому фазовому простору. Незалежно від конкретного значення початкової точки розв'язки системи "блукають" зовнішньо хаотичним (але повністю детермінованим) чином по усьому фазовому простору, не виявляючи періодичності. Стан системи (3), коли дивний аттрактор асоціюється з усим припустимим фазовим об'ємом, покладено в основу нового генератора ПВЧ. Він являє собою алгоритм формування двійкової послідовності шляхом символічного опису всього фазового простору (тобто "розмитого" дивного аттрактора), розділеного довільним чином на дві рівні (за площею) частини.

Як показало дослідження нового алгоритму за допомогою системи емпіричних тестів, генератор формує псевдовипадкову числову послідовність, що характеризується високими статистичними якостями. Прийнятна швидкість роботи, простота технічної реалізації алгоритму дозволяють використовувати його у відповідальних системах потокового шифрування.

У третій главі "Розробка методів таймерного канального кодування" запропоновано підхід до побудови і реалізації високоефективних кодів з обмеженими довжинами серій, що базується на концепції представлення та обробки інформації в таймерному вигляді; на його основі розроблено методи канального кодування і способи ЦМЗ, які забезпечують значне підвищення рівня інформаційної безпеки та поліпшення технічних характеристик систем цифрового запису і зв'язку.

Таймерна ідеологія, що лежить в основі цілого класу засобів обчислювальної техніки, застосовує час як операційний параметр таймерних обчислювальних пристроїв та систем. Подання інформації у вигляді часових інтервалів певної тривалості дозволяє підвищити ефективність її обробки та передачі. Тому є підстави використати принципи таймерного кодування для розробки нових способів цифрового запису з поліпшеними технічними характеристиками.

Відомо, що застосування таймерного розрядно-аналогового кодування веде до підвищення завадозахищеності інформації, і це можна показати шляхом розрахунку коефіцієнта толерантності. Останній характеризує стійкість до спотворення в групі старших розрядів і при розбитті початкової розрядної послідовності на повні групи довжиною k з таймерним поданням інформації усередині кожної із них дорівнює

$$T(k) = k \cdot 2^{k-1} / (2^k - 1). \qquad (4)$$

У дисертаційній роботі стосовно ЗЗП, коли треба забезпечити компроміс між завадозахищеністю інформації і довжиною таймерного операнда, пропонується здійснювати після розбиття початкової інформації на повні групи початкове кодування з використанням систем числення з невеликою основою r (три - сім), а вже потім кожний одержаний r-ковий розряд представляти в таймерному вигляді. При цьому коефіцієнт толерантності буде дорівнювати або наближатися до

$$T(r) = 0{,}5 \log_2 r \cdot r / (r-1). \qquad (5)$$

У системах цифрового запису для забезпечення самосинхронізації сигналів і зменшення міжсимвольної інтерференції застосовується канальне кодування, зокрема, так звані (d,k) - коди, або коди з обмеженими довжинами серій. Вони перетворюють початкову інформацію в двійкову послідовність певного вигляду, що являє собою серії "нулів", обмежені знизу (d) і зверху (k) і відокремлені поодинокими "одиницями". При цьому кількість різних безперервних серій "нулів" у перетвореній послідовності складає величину

$$r = k - d + 1. \qquad (6)$$

Автором запропоновано підхід до побудови високоефективних (d,k) - кодів на основі таймерного розрядного подання інформації. Початкова інформація по певному алгоритму відображується у послідовність чисел, представлених в позиційній системі числення із заданою основою r (r>2). Кожний розряд r-кового числа модулюється часовим інтервалом, тривалість якого відповідає числовому значенню розряда. Внаслідок подання часового інтервалу кортежем двійкових інформаційних символів, що складається з "одиниці", за якою йдуть "нулі", буде одержана двійкова послідовність, підпорядкована (d,k)-обмеженням. В термінах графів суть методу полягає у відображенні бінарного дерева комбінацій в r-арне (r>2) дерево таймерних операндів при дотримуванні заданих обмежень. Результати проведених розрахунків показують, що застосування даного підходу дозволяє значно покращити технічні характеристики ЗЗП, у першу чергу, збільшити щільність запису і підвищити надійність функціонування.

Далі в дисертаційній роботі пропонується винахід нових способів ЦМЗ. Формула винаходу включає такі три пункти.

1. Спосіб цифрового магнітного запису, що полягає в попередньому перекодуванні початкової двійкової інформаційної послідовності у послідовність чисел із заданою кількістю розрядів, формуванні з одержаної послідовності сигналів запису з тривалістю, яка тотожна інформаційним символам послідовності, і в запису одержаних

сигналів, котрий відрізняється тим, що при попередньому перекодуванні послідовність чисел подають у системі числення з основою r, більшою двох, а тривалості сигналів запису обирають тотожними інформаційним символам послідовності r-кових чисел.

2. Спосіб цифрового магнітного запису по пункту 1, котрий відрізняється тим, що при перекодуванні початкової двійкової інформаційної послідовності встановлюють для кожного інформаційного символа r-кового коду часовий інтервал t_1, де 1 = 1, 2, ..., r, поділяють початкову двійкову інформаційну послідовність на групи двійкових символів у вигляді вхідних кодових слів однакової довжини, які перекодують у вихідні кодові слова однакової довжини у вигляді груп r-кових символів, що вибираються з множини r-кових вихідних кодових слів як відповідні найкоротшим за тривалістю комбінаціям сигналів запису, при цьому необхідну для забезпечення такого вибору надмірну кількість вихідних r-кових кодових слів визначають по співвідношенню їхньої довжини до довжини вхідних двійкових кодових слів.

3. Спосіб цифрового магнітного запису по пункту 1, котрий відрізняється тим, що при перекодуванні початкової двійкової інформаційної послідовності встановлюють для кожного інформаційного символа r-кового коду часовий інтервал t_1, де 1 = 1, 2, ..., r, поділяють початкову двійкову інформаційну послідовність на групи двійкових символів у вигляді кодових слів різної довжини, які перекодують у вихідні кодові слова у вигляді груп r-кових символів, при цьому вхідним двійковим кодовим словам, що мають найбільші імовірності появи у випадковій двійковій інформаційній послідовності, присвоюють вихідні кодові слова, котрі вибираються з множини r-кових вихідних кодових слів як відповідні найкоротшим за тривалістю комбінаціям сигналів запису.

Завдяки найбільшій економічності трійкова система числення займає особливе місце в ряду позиційних систем. Її використання в обчислювальній техніці може забезпечити якісно новий рівень функціонально-обчислювальних можливостей і техніко-економічних показників (приклад - розроблена під керівництвом М.П.Брусенцова трійкова ЕОМ "Сетунь"). Відповідно до ЗЗП великий ефект досягається за рахунок поєднання трійкового і таймерного представлення інформації на рівні канального кодування. Розглянувши бінарне дерево комбінацій і триарне дерево таймерних операндів та встановивши відповідності між ними за заданими (d,k)-обмеженнями, можна побудувати новий (1,3)-код. При таймерному трійковому кодуванні (ТТК) у порів-

нянні з відомим способом з модифікованою частотною модуляцією (МЧМ) досягається відносне збільшення поздовжньої щільності запису на 9,09% і зменшення частоти перемагнічувань носія на 3,03%.

Таблиц кодування ТТК і МЧМ

(1,3)-код	Початкова група R_i (інформаційні біти)	Трійкове подання	Перетворена група G_i (канальні біти)	Умова R_{i-1}	Тривалість сигнала запису
ТТК	1 0 0 0 1	0 1 2	1 0 1 0 0 1 0 0 0		1 T 1,5 T 2 T
МЧМ	1 0 0		0 1 1 0 0 0	- 0 1	1 T 1 T 1 T

Поєднання двох принципів подання інформації - таймерності і трійковості - забезпечує значне підвищення рівня захисту інформації зовнішньої пам'яті. Висока щільність запису, завадостійкість, надійність функціонування ЗЗП у поєднанні з простотою технічної реалізації дають всі підстави для практичного застосування ТТК при створенні захищених засобів обчислювальної техніки.

У четвертій главі "Розробка технічних засобів захисту інформації ЗЗП" розроблено основи технічної реалізації нових математичних методів захисту інформації ЗЗП; створено прикладну комп'ютерну програму шифрування файлів з використанням генератора ПВЧ на основі цілочисельної математичної моделі з дивним аттрактором; запропоновано принципи організації апаратних засобів захисту інформації ЗЗП на базі нового генератора ПВЧ і метода ТТК.

Створено набір повних аналогів функцій стандартної бібліотеки Borland C++ для роботи з криптографічно якісним алгоритмом вироблення псевдовипадкових числових послідовностей. Функції дозволяють швидко розробляти ефективні програмні засоби потокового шифрування, а також легко модифікувати раніше написані програми.

В практичних цілях мовою C (Borland C++ 3.1) створено прикладну комп'ютерну програму, що в інтерактивному режимі виконує потокове шифрування будь-яких вибраних файлів з використанням генератора ПВЧ на основі цілочисельної математичної моделі з дивним аттрактором. Реалізуючи повною мірою всі переваги алгоритму, програма забезпечує високу надійність захисту інформації зовнішньої пам'яті ЕОМ.

Одержані результати дозволяють використати програмну розробку

також при створенні надійних утиліт шифрування даних в реальному часі та інтегрованих програмних систем захисту інформації ЗЗП.

Далі в дисертації розглядаються можливості технічної реалізації на апаратному рівні створених математичних методів захисту інформації ЗЗП. Пропонуються принципи організації ряду пристроїв, в тому числі електронного ключа, інтелектуальної картки, формувача одноразового блокноту, адаптера накопичувача ЗЗП та інших. На прикінці роботи наведено приклади практичного застосування нових математичних методів в таймерних технічних засобах, зокрема в телефонному маскіраторі і в замку з електронним ідентифікатором особи. Вони показують великі можливості розробки перспективних апаратних засобів, що відповідають сучасним вимогам інформаційної безпеки.

У висновках сформульовані основні результати роботи.

Додатки містять алгоритми, комп'ютерні моделі і розроблені програмні засоби захисту інформації.

ВИСНОВКИ

Головний результат дисертаційної роботи полягає в створенні принципово нових підходів до технічного захисту інформації електромеханічних зовнішніх запам'ятовуючих пристроїв від загроз безпеці різноманітного характеру. Перший підхід - криптографія на основі дивних аттракторів, другий - таймерне кодування у некриптографічному захисті інформації. Розроблені в рамках запропонованих ідей та доведені до практичного застосування математичні методи і технічні засоби в комплексі дозволяють забезпечити високий рівень інформаційної безпеки.

У ході роботи одержані такі основні наукові результати.

1. На основі аналізу математичних методів і технічних засобів захисту інформації ЗЗП виконано формалізацію проблеми технічного захисту інформації зовнішньої пам'яті у вигляді інформаційної моделі ЗЗП. Показано, що надійний захист інформації ЗЗП може бути забезпечений тільки шляхом інтеграції криптографічного і некриптографічного (у першу чергу канального) кодування.

2. Запропоновано і науково обгрунтовано використання в криптографічних цілях теорії детермінованого хаосу, що базується на концепції дивного аттрактора. Зокрема, запропоновано в системах потокового шифрування виробляти криптостійкі псевдовипадкові числові послідовності за допомогою математичних моделей з дивними аттракторами.

3. Розроблено і програмно реалізовано систему емпіричних тес-

тів, яка дозволяє скласти комплексну оцінку властивостей генератора ПВЧ, орієнтованого на застосування в криптографічному захисті інформації. Система включає перевірку довжини періоду, оцінку частот, виявлення тренда, кореляційний аналіз, визначення лінійної складності псевдовипадкової числової послідовності, що формується. Показано неспроможність відомих алгоритмів вироблення ПВЧ (лінійного конгруентного алгоритму і метода на основі лінійного регістра зсуву із зворотним зв'язком) у розв'язанні задач криптографії.

4. За допомогою обчислювальних експериментів з відомими математичними моделями Лоренца і Хенона доведено принципову можливість побудови криптографічно якісних джерел випадкових і псевдовипадкових числових послідовностей на основі дивних аттракторів. Побудовані генератори ПВЧ являють собою алгоритми вироблення двійкової послідовності шляхом символічного опису аттрактора (Лоренца або Хенона) з наступною її децимацією по індексу 7.

5. Побудовано і досліджено нову, цілочисельну математичну модель динамічної системи з дивним аттрактором. Стан системи, коли дивний аттрактор асоціюється з усим допустимим фазовим об'ємом, покладено в основу нового генератора ПВЧ. Розроблений генератор формує псевдовипадкову двійкову послідовність, що характеризується високими статистичними якостями. Прийнятна швидкість роботи, простота технічної реалізації алгоритму дозволяють використовувати його у відповідальних системах потокового шифрування.

6. Запропоновано використання в системах ЦМЗ принципів подання інформації в таймерному вигляді і її обробки за допомогою таймерних обчислювальних пристроїв. Шляхом розрахунку коефіцієнта толерантності показано, що таймерне розрядно-аналогове кодування в поєднанні з перетворенням в системах числення з невеликою основою (три - сім) забезпечує підвищення завадозахищеності інформації ЗЗП і при цьому не веде до значного збільшення довжини таймерних операндів.

7. Розроблено метод побудови кодів з обмеженими довжинами серій на основі таймерного розрядного представлення інформації, застосування якого дозволяє значно покращити технічні характеристики ЗЗП. В термінах графів суть методу полягає у відображенні бінарного дерева комбінацій в r-арне (r>2) дерево таймерних операндів при дотримуванні заданих обмежень.

8. Запропоновано ряд нових способів ЦМЗ, що забезпечують значне підвищення щільності запису за рахунок поєднання таймерних

принципів представлення інформації з перекодуванням в системах числення з основою більше двох. Позитивний технічний результат досягається тим, що кожний із способів включає перекодування початкової двійкової інформації в послідовність r-кових чисел (r>2) із заданою кількістю розрядів і формування сигналів запису з тривалістю, яка тотожна інформаційним символам одержаної послідовності. Винахід "Спосіб цифрового магнітного запису", одним з авторів якого є дисертант, захищено патентом Російської Федерації.

9. Створено метод таймерного трійкового кодування, завдяки якому можливе значне підвищення рівня некриптографічного захисту інформації в системах цифрового запису і зв'язку, в тому числі збільшення щільності запису, швидкості передачі, завадозахищеності, надійності функціонування. Це поряд з простотою технічної реалізації є підставою для практичного застосування ТТК при створенні захищених засобів обчислювальної техніки.

10. Розроблено основи технічної (програмної і апаратної) реалізації нових математичних методів захисту інформації ЗЗП. Створено прикладну комп'ютерну програму шифрування файлів з використанням генератора ПВЧ на основі цілочисельної математичної моделі з дивним аттрактором. Запропоновано принципи організації апаратних засобів захисту інформації ЗЗП на базі нового генератора ПВЧ і метода ТТК.

Основні положення дисертації опубліковані в таких працях:

1. Пономарев А.А. Псевдослучайные числа в криптографических системах // Математические методы в компьютерных системах. - Киев: Ин-т кибернетики им. В.М.Глушкова НАН Украины, 1996.- С.60-69.

2. Пономарев А.А. Способы цифровой магнитной записи, основанные на групповом кодировании // Математические методы и программные средства в научных исследованиях. - Киев: Ин-т кибернетики им. В.М.Глушкова НАН Украины, 1994.- С.101-108.

3. Пономарев А.А. Методические указания по изучению компьютерной вирусологии / АН Украины. Научно-учебный центр прикладной информатики; Отв. ред. Гупал А.М. - Киев: Ин-т кибернетики им. В.М.Глушкова АН Украины, 1993.- 54 с.

4. Гупал А.М., Пономарев А.А., Цветков А.М. Об одном методе индуктивного вывода с подрезанием деревьев решений // Кибернетика и системный анализ.- 1993.- N 5.- С.174-178.

5. Гупал А.М., Пономарев А.А., Цветков А.М. Методические указания по изучению экспертных систем / АН Украины. Научно-

учебный центр прикладной информатики; Отв. ред. Михалевич М.В. - Киев: Ин-т кибернетики им. В.М.Глушкова АН Украины, 1993.- 48 с.

6. Пономарев А.А. Аттрактор Лоренца в обеспечении конфиденциальности информации // Тез. докл. VII Украинской конф. "Моделирование и исследование устойчивости систем". Секция "Моделирование систем".- Киев, 1996.- С.111.

7. Пономарев А.А. Таймерное кодирование и защита информации внешних запоминающих устройств // Праці Третьої української конф. з автоматичного керування ("Автоматика-96").- Севастополь: СевГТУ, 1996.- Т.1.- С.219.

8. Бардаченко В.Ф., Пономарев А.А. Принципы разработки таймерных канальных кодов, повышающих емкость внешних запоминающих устройств // Праці Другої української конф. з автоматичного керування ("Автоматика-95").- Львів: НВЦ "ІТІС", 1995.- Т.4.- С.40-41.

9. Бардаченко В.Ф., Пономарев А.А. Разработка внешних запоминающих устройств с улучшенными техническими характеристиками на базе применения систем счисления с основаниями свыше двух // Матеріали наук.-метод. конф. "Програмно-технічні засоби інформатизації освіти": Тези доп.- Київ: ІСДО, 1995.- С.80-81.

10. Бардаченко В.Ф., Пономарев А.А., Шурчков И.О., Немудров В.Г. Способ цифровой магнитной записи. Патент Российской Федерации, МПК G11B 5/09, 1997.

11. Бардаченко В.Ф., Пономарев А.А. Методы таймерного кодирования информации // Разработка таймерных вычислительных устройств систем автоматизированного управления и информатики: (Заключ. отчет о НИР) / Центр таймерных вычислительных систем Ин-та кибернетики им. В.М.Глушкова НАН Украины; Руководитель темы В.Ф.Бардаченко.- N ГР 0194U006283.- Киев, 1995.- С.10-24.

12. Распределенные многопользовательские таймерные информационные системы в энергетике // Разработка аппаратно-программных средств обеспечения распределенных таймерных информационно-вычислительных систем для автоматизации производственных процессов в энергетике на базе ПЭВМ и компьютерных платформ типа AS/400, PS/VP, PS/1 (БАЗА-94) / В.Ф.Бардаченко, А.А.Пономарев, В.И.Вешняков и др.: (Заключ. отчет о НИР) / Центр таймерных вычислительных систем Ин-та кибернетики им. В.М.Глушкова НАН Украины; Руководитель темы В.Ф.Бардаченко.- N ГР 0195U005979.- Киев, 1994.- С.35-51.

Пономарев А. А. Математические методы и технические средства защиты информации внешних запоминающих устройств.

Диссертация на соискание ученой степени кандидата физико-математических наук по специальности 01.05.03 — математическое и программное обеспечение вычислительных машин и систем, Институт кибернетики им. В. М. Глушкова НАН Украины, Киев, 1997.

Диссертация содержит теоретические исследования в области технической защиты информации. Применительно к электромеханическим внешним запоминающим устройствам предложены принципиально новые подходы к обеспечению информационной безопасности: странные аттракторы в криптографической защите и таймерное кодирование в некриптографической защите информации. В плане развития указанных идей создан ряд математических методов и алгоритмов, включая криптографически качественный генератор псевдослучайных чисел и метод таймерного троичного кодирования, разработаны основы их программной и аппаратной реализации.

Ponomariov A. A. Mathematical Methods and Technical Means of Protection of the Information of External Storage Devices.

The dissertation is presented for academic degree of candidate of physical and mathematical sciences in speciality 01.05.03 — Mathematical support and software of computers and computer systems, V. M. Glushkov Institute of cybernetics, National academy of sciences, Ukraine, Kiev, 1997.

The dissertation contains theoretical researches in the field of technical protection of the information. With reference to electro-mechanical external storage devices the principle new approaches to ensuring of information safety are suggested: strange attractors in cryptographic protection and timer coding in non-cryptographic protection of the information. In the plan of development of the specified ideas a number of mathematical methods and algorithms is created, including the cryptographicly qualitative generator of pseudo-random numbers and method of timer ternary coding, bases of their software and hardware realization are worked out.

Ключові слова: захист інформації, зовнішній запам'ятовуючий пристрій, дивний аттрактор, таймерне кодування.

Підп. до друку 03.04.97. Формат 60×84/16. Папір офс. Офс. друк. Ум. друк. арк. 0,93. Ум. фарбо-відб. 1,16. Обл.-вид. арк. 1,0. Зам. 127. Тираж 100 прим.

Редакційно-видавничий відділ з поліграфічною дільницею
Інституту кібернетики імені В. М. Глушкова НАН України
252022 Київ 22, проспект Академіка Глушкова, 40