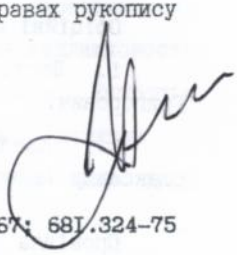
МІНІСТЕРСТВО ОСВІТИ УКРАЇНИ

ХАРКІВСЬКИЙ ДЕРЖАВНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

РАДІОЕЛЕКТРОНІКИ

На правах рукопису



АЛІПОВ ІЛЛЯ МИКОЛАЙОВИЧ

УДК 681.324.067: 681.324-75

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ЇЇ ПЕРЕДАВАННІ

05.13.08 – Обчислювальні машини, системи та мережі, елементи і пристрої обчислювальної техніки та систем керування

Автореферат дисертації

на здобуття наукового ступеня

кандидата технічних наук

Харків-1997

04.03

Дисертація є рукопис.

Робота виконана на кафедрі автоматизації проектування обчислювальної техніки Харківського державного технічного університету радіоелектроніки.

Науковий керівник - кандидат технічних наук, професор Какурін Микола Яковлевич.

Офіційні опоненти:

1. Доктор технічних наук, професор Руденко Олег Григорович.

2. Кандидат технічних наук, доцент Тимченко Олександр Іванович.

Провідна організація -Харківський авіаційний інститут ім М.Є.Жуковського, Міністерство освіти України, м.Харків.

Захист дисертації відбудеться "14" лютого 1997 р. на засіданні спеціалізованої вченої ради К 02.25.03 у Харківському державному технічному університеті радіоелектроніки за адресою: 310726, м. Харків, пр. Леніна, 14.

З дисертацією можна ознайомитись у бібліотеці Харківського державного технічного університету радіоелектроніки за адресою: 310726, м. Харків, пр. Леніна, 14.

Автореферат розіслано "13" червня 1997 року.

Вчений секретар
спеціалізованої вченої ради Безкоровайний В.В.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

АКТУАЛЬНІСТЬ. Створення ЕОМ і їх використання в будь-яких галузях науки і техніки привело до нової проблеми - захист інформації при її передачі і зберіганні. Ця проблема зараз вирішується в цілому за рахунок використовування криптографічних методів (підстановок, перестановок, адитивних методів), які націлені на зменшення надлишковості відкритого тексту та збільшення ентропії ключа. Ентропія ключа збільшується за рахунок змінювання довжини і збільшення циклів шифрування. Але цей підхід не може бути використаний для шифрування коротких запитів. Крім того, методи захисту інформації завжди повинні удосконалюватися (проблема захисту інформації - вічна проблема). Одним з таких напрямків удосконалення методів захисту інформації є напрямок, пов'язаний з використанням теорії скінченних автоматів з псевдовипадковими переходами з одного стану до іншого. Але до цього часу такі методи захисту інформації не розвинуті.

Таким чином, важливим і актуальним є створення на основі деревоподібних автоматів систем пошуку точки на відрізку одиничної довжини (точки екстремуму унімодальної функції) і оригінальних криптографічних методів захисту інформації.

ОБ'ЄКТОМ ДОСЛІДЖЕННЯ є система захисту інформації в ЕОМ при її передачі і зберіганні, яка побудована на базі завадостійких до віртуальних завад алгоритмів пошуку точки екстремуму унімодальної функції.

ПРЕДМЕТ ДОСЛІДЖЕНЬ полягає у підвищенні ентропії ключа за рахунок псевдовипадкової зміни його довжини та псевдови-

падкового вибору конкретного значення ключа для окремого символу, що належить деякій множині.

МЕТОЮ ДИСЕРТАЦІЙНОЇ РОБОТИ є розробка і дослідження методів захисту інформації в ЕОМ при її передачі і зберіганні на основі завадостійких до віртуальних завад алгоритмів пошуку точки екстремуму унімодальної функції.

МЕТОДИ ДОСЛІДЖЕНЬ. В роботі були використані методи теорії графів, скінченних автоматів, множин, алгоритмів і алгебри логіки.

ЗАДЛЯ ДОСЯГНЕННЯ МЕТИ БУЛИ ПОСТАВЛЕНІ Й ВИРІШЕНІ СЛІДУЮЧІ ЗАДАЧІ:

1. Синтез оптимальних завадостійких до віртуальних A_1, A_2- послідовностей алгоритмів пошуку точки екстремуму унімодальної функції.

2. Синтез логічно нескладних завадостійких до A_1,A_2- послідовностей алгоритмів одновимірного пошуку точки екстремуму унімодальної функції.

3. Розробка і дослідження на основі завадостійких до A_1,A_2- послідовностей алгоритмів одновимірного пошуку точки екстремуму унімодальної функції нових методів захисту інформації, які підвищують ентропію ключа.

4. Побудова на основі завадостійких алгоритмів методів захисту інформації від несанкціонованого доступу (НСД) і дії випадкових завад у каналі.

5. Розробка структурних схем кодуючих та декодуючих пристроїв дискретного каналу передачі інформації для синтезованих методів захисту інформації.

НАУКОВА І ПРАКТИЧНА НОВИЗНА положень та результатів дисертаційної роботи полягає у тому, що вперше:

1. Синтезовано оптимальні завадостійкі до віртуальних A_1, A_2-послідовностей алгоритми одномірного пошуку точки екстремуму унімодальної функції для а-схем.

2. Створено логічно нескладні завадостійкі до A_1, A_2-послідовностей алгоритми одномірного пошуку точки екстремуму унімодальної функції для а-схем.

3. Наведено приклади формування оптимальних і логічно нескладних завадостійких до A_1, A_2-послідовностей алгоритмів одномірного пошуку точки екстремуму унімодальної функції для а- схем.

4. Синтезовано методи генерації псевдовипадкових послідовностей для символів вхідного алфавіту (методи підстановок) на основі завадостійких до A_1,A_2-послідовностей алгоритмів пошуку.

5. Синтезовано на основі надлишкових систем зображення десяткових чисел методи захисту інформації від НСД і дії в каналі випадкових завад.

6. Створено імітаційну модель для дослідження методів захисту інформації на основі завадостійких алгоритмів пошуку.

7. Розроблено структурні схеми кодуючих і декодуючих пристроїв дискретного каналу передачі інформації для методів захисту інформації на основі завадостійких алгоритмів пошуку та нових надлишкових систем зображення десяткових чисел, побудованих на основі оцінок завадостійких алгоритмів пошуку.

8. Синтезовано нові генератори псевдовипадкових послідовностей ключів для методу підстановок, які дозволяють псевдовипадковим чином змінювати довжину ключа і його зна-

чення, що значно збільшує ентропію ключа.

9. Розроблено на основі оцінок завадостійких алгоритмів пошуку надлишкові зображення десяткових чисел, які не тільки захищають інформацію від НСД, але й від дії випадкових завад в дискретному каналі.

НА ЗАХИСТ ВИНОСЯТЬСЯ СЛІДУЮЧІ ПОЛОЖЕННЯ:

I. Оптимальні завадостійкі до віртуальних A_1, A_2- послідовностей алгоритми одновимірного пошуку точки екстремуму унімодальної функції.

2. Завадостійкі логічно нескладні алгоритми одновимірного пошуку точки екстремуму унімодальної функції.

3. Конкретні завадостійкі до A_1, A_2- послідовностей алгоритми одномірного пошуку.

4. Співвідношення для вирішуючої функції пошуку, які дозволяють виділити новий інтервал невизначеності і розподілити точки наступного експерименту.

5. Генератори псевдовипадкових ключів для методу підстановок, які дозволяють псевдовипадковим чином змінювати довжину ключа та його значення.

6. Надлишкові зображення десяткових чисел, на основі яких синтезуються методи захисту інформації від НСД і від випадкових завад, які діють у дискретному каналі передачі інформації.

7. Структурні схеми кодуючих і декодуючих пристроїв дискретного каналу передачі інформації для методів захисту інформації, які синтезовані на основі завадостійких алгоритмів.

РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ. Результати роботи отримані та реалізовані в процесі виконання держбюджетних НДР по

створенню нових методів захисту інформації при її передачі, а також використовуються в навчальному процесі при виконанні лабораторних робіт і в дипломному проектуванні (створено діючий макет кодуючого і декодуючого пристроїв дискретного каналу передачі інформації).

АПРОБАЦІЯ РОБОТИ ТА ПУБЛІКАЦІЇ. Основні положення і результати дисертаційної роботи доповідались та обговорювались на двох міжнародних конференціях "Теория и техника передачи, приема и обработки информации" (Харків-Туапсе, 1995 р., 1996 р.).

ПУБЛІКАЦІЇ. Зміст роботи досить повно відображено у шістнадцяти публікаціях.

СТРУКТУРА І ОБСЯГ РОБОТИ. Дисертація має у своєму складі вступ, чотири розділи й закінчення, викладені на 125 сторінках, містить 1 додаток, 10 малюнків, 6 таблиць та бібліографію з 87 назв.

ЗМІСТ РОБОТИ

У вступі стисло освітлено предмет дослідження, обгрунтовано актуальність теми, дано загальну характеристику роботи. Викладено мету дослідження; задачі, що розв'язуються; загальні положення, які виносяться на захист; наукову новизну та практичну цінність результатів.

У першому розділі виконано аналітичний огляд існуючих методів захисту інформації, який виявив, що в галузі розробки методів захисту інформації є ряд невирішених проблем. А саме: існуючі системи захисту інформації в основному реалізують методи, пов'язані зі зменшенням надлишковості повідомлення, що передається. Методи захисту інформації, які збільшують ентропію ключа недостатньо розвинуті. Одним з перспек-

тивних напрямків у розвитку криптографії є напрямок, пов'язаний з використанням деревоподібних дискретних автоматів з псевдовипадковими переходами із одного стану в інший. Деревоподібні автомати з псевдовипадковими переходами задаються алгоритмами завадостійкого пошуку. У теорії завадостійкого пошуку точки екстремуму унімодальної функції вирішена тільки одна задача: узагальнення алгоритму Кіфера для, так званих, б-схем алгоритмів. Для а-схем не існує рішень навіть для окремих випадків.

Все сказане обумовило вищеперелічені задачі дослідження.

У другому розділі наведено розв'язання задачі синтезу оптимальних завадостійких до віртуальних A_1, A_2- послідовностей алгоритмів пошуку точки екстремуму унімодальної функції.

Для опису задач дослідження в термінах теорії пошуку введено ряд понять та визначень, використано принцип "повторних порівнянь"; модифіковано відомий принцип "перехрещення" (принцип алгоритмічного придушення віртуальних завад, які накладаються на процес пошуку точки екстремуму унімодальної функції).

Алгоритми пошуку характеризуються довжиною пошуку (кількістю кроків алгоритму) та кількістю точок експерименту, які формуються одночасно (одночасно формуються k точок експерименту). Точка екстремуму x^* належить відрізку одиничної довжини (відрізку $[0,1]$. Під експериментом розуміють визначення істинності предикату:

$$P\left\{f_j\left(x_\beta^j\right) = \max_{\rho=\overline{1,k}}\left\{f_j\left(x_\rho^j\right)\right\}\right\}, \qquad (1)$$

де $f_j\left(x_\rho^j\right)$ – значення функції $f(x)$ у точці x_ρ^j, яке сформоване

або підраховане в умовах дії завад; x_ρ^j - точка експерименту на j-му кроці алгоритму, $\rho=\overline{1,k}$; j - номер кроку алгоритму, $j=\overline{1,I}$.

Під кроком алгоритму пошуку точки x^* розуміють виконання сукупності дій: здійснення експерименту у k його точках і виділення нового інтервалу невизначеності відносно x^*. Ці дії виконуються за допомогою вирішуючих функцій d_j^1 і d_j^2. Ефективність алгоритмів пошуку x^* оцінюється довжиною інтервалу невизначеності, який отримано на останньому кроці алгоритму. Ця довжина залежить від функції $f(x)$ та від обраного алгоритму. Тому, оцінкою ефективності z_1-го алгоритму є величина

$$L_{z_1} = \max_{f\in F} \left\{ l_1\left(f, z_1\right)\right\} + \varepsilon , \qquad (2)$$

де ε - найменша допустима відстань між двома сусідніми точками експериментів; $l_1\left(f, z_1\right)$ - довжина інтервалу невизначеності, який одержано на останньому кроці z_1-го алгоритму; F-множина унімодальних функцій.

Оптимальним алгоритмом названо алгоритм, для якого справедливо співвідношення:

$$\max_{f\in F} l_1\left(f, z_1^*\right) \leqslant \min_{z_1\in M_1} \max_{f\in F} \left(f, z_1\right) + \varepsilon, \qquad (3)$$

де M_1 - множина можливих алгоритмів.

Зворотня величина від L_{z_1} позначена сукупністю символів $\Phi_{z_1}(1,k)$, яка Стаховим А.П. названа (1,k)-точністю.

Стратегія пошуку S_j однозначно задається розбиванням вихідного напіввідкритого інтервалу невизначеності $\left[x_{q_{j-1}}^{j-1,1}-1, x_{q_{j-1}}^{j-1,2}+1\right)$ на k напіввідкритих інтервалів, які перехрещуються:

$$A_j = \left\{\left[x^{j-1,1}_{q_{j-1}}, x^j_2\right], \left[x^j_2, x^j_3\right], \ldots, \left[x^j_k, x^{j,2}_{q_{j-1}+1}\right]\right\}. \quad (4)$$

Розглядаються віртуальні завади однополярні (A_1- послідовності) і двополярні (A_2- послідовності). Кожну послідовність описує сукупність параметрів a,l,H, де a - максимально можливе значення амплітуди завади; l - максимально можливе значення тривалості завади; H - мінімально можливе значення інтервалу між двома сусідніми віртуальними завадами.

Задача синтезу алгоритмів, оптимальних до віртуальних завад у вигляді A_1, A_2- послідовностей, формулюється так, як описано нижче.

Дано клас F таких унімодальних функцій однієї змінної, для яких:

$$f: I \to R,\ I \in [0,1],\quad f(x^*) = \max_x f(x),\ x^* \in [0,1].$$

Точка x^* в процесі пошуку її координати не змінює свого положення, на процес пошуку накладається тільки $A_\nu(a,l,H)$-послідовність (ν=1,2).

Пошук x^* здійснюється алгоритмом, який складається з i кроків і формує одночасно k точок експериментів. Експеримент на j-му кроці алгоритму описується розбиванням $\left[\tilde{x}^{j-1}_{q_{(j-1)}-1}, \tilde{x}^{j-1}_{q_{(j-1)}+1}\right]$ на k нових напіввідкритих інтервалів:

$$A_j = \left\{\left[\tilde{x}^{j-1}_{q_{(j-1)}-1}, x^1_2\right], \left[x^j_1, x^j_3\right], \ldots, \left[x^j_{k-1}, \tilde{x}^{j-1}_{q_{(j-1)}+1}\right]\right\}, \quad (5)$$

де $x^* \in \left[\tilde{x}^{j-1}_{q_{(j-1)}-1}, \tilde{x}^{j-1}_{q_{(j-1)}+1}\right]$, і полягає спочатку в спостереженні (обчисленні або формулюванні) $f_j\left(x^j_{q_1}\right)$, де $q_1 = \overline{1,k}$, $x^j_{q_1}$ - q_1-а точка експерименту на j-му кроці алгоритму; $x^j_{q_1} \in \left[\tilde{x}^{j-1}_{q_{(j-1)}-1}, \tilde{x}^{j-1}_{q_{(j-1)}+1}\right]$, а потім - у знаходженні

$$f_j\left(x^j_q\right) = \max_{q_1} f_j\left(x^j_{q_1}\right). \qquad (6)$$

Множиною значень експериметів, вільних від помилок, є множина z={1,2,...,k}, елементи якої формуються у відповідності з правилом:

$$\varepsilon_{A_j[f(x),k]} = q: \Leftrightarrow f\left(x^j_q\right) = \max_{\rho} f\left(x^j_\rho\right), \qquad (7)$$

де $q \in z$; $\varepsilon_{A_j[f(x),k]}$ – умовний запис елемента q множини z, що задана на розбиванні A_j, яке в свою чергу залежить від функції f та кількості точок експерименту k, що формуються одночасно.

Під дією імпульсних завад замість εA_j будемо спостерігати випадкові величини

$$Y_{A_j}\left[f(x),A_\nu(a,l,H),h\right] = Y_j \in Z=\{1,2,\ldots,k\}. \qquad (8)$$

Вирішальні функції d^1_j и d^2_j формують інтервал невизначеності відносно x^* відповідно на j-му і (j-l-1)-му кроках алгоритму:

$$d^1_j: Y_j \to A_j,\ \left[x^j_{q_j-1}, x^j_{q_j+1}\right] \subset \left[\overset{\approx}{x}{}^j_{q_j-1}, \tilde{x}^j_{q_j+1}\right] \subset A^1_j;$$
$$d^2_j: \left\{Y_{j-l-1}, Y_{j-l}, \ldots, Y_j\right\} \to A_{j-l-1}, \qquad (9)$$

де $\left[\overset{\approx}{x}{}^j_{q_j-1}, \tilde{x}^j_{q_j+1}\right]$-напіввідкритий інтервал невизначеності відносно x^*, який сформовано на основі Y_j функцією d^1_j; d^2_j - функція, яка встановлює на основі послідовності випадкових величин, що містить (l+1)-й член, справедливість зробленого на (j-l-1)-му кроці алгоритму висновку про інтервал невизначеності відносно x^*.

Задача полягає в тому, щоб для будь-яких $l>1$, $k \geqslant 1$, $\varepsilon>0$ (ε- мінімально допустима відстань між точками двох сусідніх

експериментів), що задані параметрами $A_\nu(a,1,H)$-послідовності, синтезувати завадостійкий алгоритм пошуку (знайти такі d_j^1, d_j^2, A_j, A_j^1), для якого має місце ε-мінімальна стратегія:

$$\max_{f\in F} l_i(f,z_1^*) \leqslant \min_{z_1\in M_1} \max_{f\in P} l_i(f,z_1)+\varepsilon \ . \qquad (10)$$

В роботі знайдені співвідношення для вирішуючих функцій d_j^1 і d_j^2, які дозволяють синтезувати оптимальні алгоритми, завадостійкі до віртуальної A_1- послідовності позитивної полярності.

Стратегія пошуку будується на положеннях, які приведені нижче. Якщо можливо без зміни (1,k)-точності алгоритму розмістити точки наступного експерименту в інтервалі $\left(x_{q-1}^j, x_{\rho_1}^{j+z}\right)$, то їх там і розміщують (оптимістична стратегія). Якщо розміщення точок наступного (j+z+1)-го експерименту в інтервалі $\left(x_{q-1}^j, x_{\rho_1}^{j+z}\right)$ зменшує (1,k)-точність алгоритму, то приймають змішану стратегію, а саме: k_1-точку розміщують в інтервалі $\left(x_{q-1}^{j,1}, x_{q-1}^j\right)$, а частину, яка залишилася,- в інтервалі $\left(x_{q-1}^j, x_{\rho_1}^{j+z}\right)$.

Показано, що оптимістична стратегія на (j+z+1)-му кроці приймається у тому випадку, коли має місце співвідношення:

$$\left(x_{q-1}^j - x_{q-1}^{j,1}\right) \leqslant h\left\{\left\{\left(\Psi(1,k)-1\right)\Psi_1^{1,H}(1-H_1-j,k)\sum_{n=2}^{H_1-z}\Psi(H_1-z-n,k)\right\} + \right.$$
$$\left. + \Psi_1^{1,H}(1-H_1-j,k)\right\} - h \qquad (11)$$

де $\Psi(1,k)$, $\Psi(H_1-z-n,k)$-оцінки оптимального відповідно трьохкрокового та (H_1-z-n)- крокового алгоритмів; $\Psi_1^{1,H}(1-H_1-j,k)$-оцінка завадостійкого $(1-H_1-j)$- крокового алгоритму;

$$H_1 = \begin{cases} H, & \text{якщо } 1-j-H\geqslant 0; \\ 1-j, & \text{якщо } 1-j-H<0. \end{cases}$$

Подібні співвідношення отримані для вибору змішаної стратегії. Схема побудови вирішуючих функцій та стратегії пошуку покладена в основу алгоритму синтезу оптимальних завадостійких до A_1- послідовностей алгоритмів.

У роботі отримані такі співвідношення, які визначають вирішуючі функції та стратегію пошуку для побудови оптимальних завадостійких до A_2-послідовностей алгоритмів пошуку точки екстремуму унімодальної функції, на основі яких визначений алгоритм синтезу оптимальних завадостійких до віртуальних A_2-послідовностей алгоритмів пошуку точки екстремуму унімодальної функції.

Наведено приклади побудови оптимальних завадостійких до A_1-послідовностей алгоритми пошуку.

Синтезовані у другому розділі завадостійкі алгоритми пошуку точки екстремуму унімодальної функції мають значну логічну складність, що дозволяє їх використовувати для захисту цінної інформації при її передаванні в дискретному каналі. При захисті менш цінної інформації необхідно використовувати більш прості завадостійкі алгоритми.

У третьому розділі наведені рішення задач синтезу завадостійких алгоритмів пошуку точки екстремуму унімодальної функції, які мають незначну логічну складність. Такі алгоритми названо П-алгоритмами. $П_1$-алгоритми завадостійкі до A_1-послідовності, а $П_2$-алгоритми - до A_2-послідовності. В основу П-алгоритмів закладено тільки принцип "повторних порівнянь".

Аналіз усіх можливих результатів, які виникають під час функціонування П-алгоритму, дав можливість для конкретної віртуальної послідовності визначити правило побудови

вирішуючих функцій та стратегій пошуку. Це дало можливість одержати схеми для вирішення задач синтезу Π_1 та Π_2-алгоритмів, на основі яких одержано конкретні Π_1 та Π_2-алгоритми та їх оцінки у вигляді функції $\Phi_1^{\ell,H}(1,3)$ і $\Phi_1^{\ell,H}(1,3)$. Оцінки Π_1 та Π_2-алгоритмів використані при побудові надлишкових зображень десяткових чисел.

У четвертому розділі розроблено на основі синтезованих у другому та третьому розділах завадостійких алгоритмів пошуку точки екстремуму унімодальної функції методи та системотехнічні засоби захисту інформації у дискретному каналі та проведено їх дослідження.

Завадостійкий алгоритм пошуку, як це було показано, дозволяє для відомої віртуальної послідовності замкнути точку екстремуму унімодальної функції в інтервал невизначеності найменшої довжини і отримати цифровий еквівалент координати цієї точки.

Такі алгоритми можна також використовувати в іграх при угадуванні задуманого числа, яке підсумовується з випадковим числом (теорія запитальників). Ця властивість завадостійких алгоритмів, виділяти задумане число з його суміші з випадковим числом, можна використовувати при захисті інформації у дискретному каналі. З цією метою усі символи, наприклад, російського алфавіту та цифри двійкової системи числення однозначно ототожнюємо з цілими позитивними числами із ряду 0, 1,...,M, де M – кількість різних символів вхідного алвафіту та цифр системи числення. Сформуємо послідовність чисел $\zeta_1,\zeta_2,\zeta_3,\dots\ \dots,\zeta_i$, де i – кількість кроків Π_1-алгоритму, датчиком псевдовипадкових чисел. Отриману таким чином псевдовипадкову послідовність обробимо, наприклад, Π_1-алгорит-

мом, який одночасно формує три точки експерименту x_1^1, x_2^1, x_3^1, які належать інтервалу (0,M). Оскільки під дією псевдовипадкового числа ζ_1 початковий інтервал невизначеності (0,M) перетворюється в інтервал (0+ζ,M+ζ), то значення унімодальної функції f(x), знайдене у точках $x_\rho^i \in (0,M)$, $\rho=\overline{1,3}$, буде відрізнятися від реальних значень цієї функції у точках $\left(x_\rho^1+\zeta_1\right)$, тому результат експерименту Y_j буде псевдовипадковим числом.

У результаті угадування числа при псевдовипадковій зміні початкового інтервалу невизначеності отримують кодову послідовність $Y_1,Y_2,Y_3,\ldots,Y_i$, яку передають по дискретному каналу. Конкретний вигляд цієї кодової послідовності визначається тими викривленнями, які вносить датчик псевдовипадкових чисел. Поскільки викривлення початкового інтервалу невизначеності з'являється псевдовипадковим чином, то і розподіл нулів, одиниць та двійок в кодовій послідовності буде також псевдовипадковим. Псевдовипадковість кодової комбінації, сформованої $П_1$-алгоритмом, є важливою властивістю, яка захищає їх при передачі по дискретному каналу.

Крім цього кодові послідовності, які переводять дискретний автомат, який задано завадостійким алгоритмом пошуку з початкового стану в один із його кінцевих станів (автомат має M кінцевих станів) мають різну довжину.

Багатообразність кодових комбінацій, які переводять дискретний автомат з початкового в один із його кінцевих станів, псевдовипадковий характер їх формування та їх нерівнозначність є важливими якостями, які дозволяють на основі таких дискретних автоматів будувати захищені дискретні канали передачі інформації.

На основі оцінок завадостійких алгоритмів пошуку побудовані надлишкові зображення десяткових чисел. Надлишковість цих зображень та їх незвичайність може бути використана для захисту інформації в дискретному каналі (кожний завадостійкий алгоритм пошуку народжує своє надлишкове зображення десяткових чисел, яке визначається параметрами віртуальної послідовності). Важливою додатковою властивістю синтезованих представлень десяткових чисел є також і те, що множина комбінацій, які відповідають конкретному десятковому числу, складається із підмножини комбінацій, які містять парну кількість одиниць у своєму зображенні, та підмножини комбінацій, які містять непарну кількість одиниць у своєму зображенні. Ця властивість використовується для підвищення завадостійкості при передачі по дискретному каналу. Тому, захист інформації при її передачі по дискретному каналу забезпечується також і зображенням десяткових чисел, що досліджується, багатообразністю для одного і того ж десяткового числа кодових комбінацій, а завадостійкість повідомлень, що передаються, - властивістю кодових повідомлень, які формуються: містити лише парну або непарну кількість одиниць у своєму зображенні.

У цьому ж розділі наведено схеми кодуючих та декодуючих пристроїв для розглянутих випадків. Побудовано лабораторний макет. Виконано дослідження запропонованих методів за допомогою імітаційного моделювання.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

В процесі виконання дисертаційної роботи одержано наступні результати:

1. Співвідношення для вирішуючої функції та стратегії

пошуку оптимальних завадостійких до A_1, A_2-послідовностей алгоритмів пошуку точки екстремуму унімодальної функції, на основі яких синтезовані завадостійкі алгоритми пошуку, які мають значну логічну складність.

2. Співвідношення для вирішуючої функції та стратегії пошуку логічно нескладних алгоритмів ($П_1, П_2$-алгоритмів), які задають дискретні автомати з псевдовипадковими переходами із одного стану в інший.

3. Конкретні завадостійкі до A_1, A_2-послідовностей алгоритми одновимірного пошуку.

4. Генератори псевдовипадкових ключів для методу підстановок на основі завадостійких до A_1, A_2-послідовностей алгоритмів одновимірного пошуку, які дозволяють псевдовипадковим чином змінювати довжину та значення ключа.

5. Надлишкові зображення десяткових чисел, на основі яких синтезовано методи захисту від НСД та дії завад у дискретному каналі.

6. Структурні схеми кодуючого та декодуючого пристроїв дисткретного каналу передачі інформації.

7. Імітаційна модель синтезованих методів захисту інформації, дослідження якої підтвердило високу надійність синтезованих методів захисту інформації.

Приведені основні результати роботи є свідченням того, що за допомогою синтезованих у роботі завадостійких алгоритмів пошуку точки екстремуму унімодальної функції розроблено нові методи захисту інформації, які збільшують ентропію ключа за рахунок псевдовипадкової зміни довжини та значення ключа при підстановках.

Дисертаційна робота є підсумком особистої роботи автора.

Основний зміст дисертації досить повно відображено у 16 роботах:

1. Алипов И.Н. Помехоустойчивые к A_1-последовательности алгоритмы поиска точки экстремума унимодальной функции // АСУ и приборы автоматики.-Харьков,ХТУРЭ.-1997.-Вып.104.-с.69-75.

2. Алипов И.Н., Ребезюк Л.Н. Помехоустойчивые к A_2- последовательности алгоритмы поиска точки экстремума унимодальной функции // АСУ и приборы автоматики.- Харьков,ХТУРЭ.- 1997.- Вып.104.-с. 123- 127.

3. Алипов И.Н., Охапкин А.А. Избыточные представления десятичных чисел на основе помехоустойчивых алгоритмов поиска // АСУ и приборы автоматики .-Харьков,ХТУРЭ.- 1997.- Вып.105.- с. 53-55.

4. Алипов И.Н., Григорьев А.В. К постановке задач синтеза помехоустойчивых и корректирующих алгоритмов одномерного поиска.- Харьков, 1995- 15 с.- Библиогр.: 4 назв.- Рус.- Деп. в ГНТБ Украины 17.07.95, №1834- Ук95.

5. Алипов И.Н., Григорьев А.В. Описание задач синтеза помехоустойчивых алгоритмов одномерного поиска.- Харьков, 1995- 11 с.- Библиогр.: 9 назв.- Рус.- Деп. в ГНТБ Украины 17.07.95, №1833- Ук95.

6. Алипов И.Н., Григорьев А.В., Литвинова Е.И. Пассивно-последовательные помехоустойчивые к $A_1(a,1,H)$ - последовательности алгоритмы поиска точки экстремума функции для подмножества a-схем.- Харьков, 1995- 12 с.- Библиогр.: 2 назв.- Рус.- Деп. в ГНТБ Украины 17.07.95, № 1835- Ук95.

7. Алипов И.Н., Ребезюк Л.Н. Пассивно-последовательные помехоустойчивые к $A_2(a,1,H)$ - последовательности алгоритмы поиска точки экстремума функции для подмножества a-схем.-

Харьков, 1995- 14 с.- Библиогр.: 2 назв.- Рус.- Деп. в ГНТБ Украины 25.07.95, №1876- Ук95.

8. Алипов И.Н., Литвинова Е.И., Ребезюк Л.Н. Примеры помехоустойчивых алгоритмов поиска.- Харьков, 1995- 14 с.- Библиогр.: 2 назв.- Рус.- Деп. в ГНТБ Украины 17.07.95, №1836- Ук95.

9. Алипов И.Н. Помехоустойчивые к $A_1(a,1,H)$- последовательности П- алгоритмы поиска точки экстремума унимодальной функции.- Харьков, 1996.-23 с.:ил.- Библиогр.: 3 назв.- Рус.- Деп. в ГНТБ Украины 21.10.96 №1927- Ук96.

10. Алипов И.Н. Помехоустойчивые к $A_2(a,1,H)$- последовательности П-алгоритмы поиска точки экстремума унимодальной функции .- Харьков, 1996.-16 с.- Библиогр.: 3 назв.- Рус.- Деп. в ГНТБ Украины 21.10.96 №1926-Ук96.

11. Алипов И.Н., Литвинова Е.И., Охапкин А.А., Ребезюк Л.Н. Генерация псевдослучайных последовательностей на основе помехоустойчивых алгоритмов поиска экстремума унимодальной функции.- Харьков, 1996.- 13 с.: ил.- Библиогр.: 2 назв.- Рус.- Деп. в ГНТБ Украины 24.10.96 №2062-Ук96.

12. Алипов И.Н., Какурин Н.Я., Ребезюк Л.Н. Избыточные представления десятичных чисел на основе помехоустойчивых алгоритмов поиска.- Харьков, 1996.- 16 с.- Библиогр.: 4 назв.- Рус.- Деп. в ГНТБ Украины.

13. Алипов И.Н., Григорьев А.В. Методы решения задач синтеза помехоустойчивых алгоритмов одномерного поиска // Международная конференция "Теория и техника передачи, приема и обработки информации"; тез.докл. / ХТУРЭ, Туапсе, 1995 - с.153.

14. Алипов И.Н., Григорьев А.В., Ребезюк Л.Н. Системы защиты

информации в дискретных каналах // Международная конференция "Теория и техника передачи, приема и обработки информации"; тез.докл. / ХТУРЭ, Туапсе, 1995- с.154.

15. Алипов И.Н., Литвинова Е.И., Ребезюк Л.Н. Генерация псевдослучайных последовательностей на основе помехоустойчивых алгоритмов поиска точки экстремума унимодальной функции // 2-я Международная конференция "Теория и техника передачи, приема и обработки информации"; тез.докл. / ХТУРЭ, Туапсе, 1996. - Часть II. с.155.

16. Алипов И.Н., Ребезюк Л.Н. Системы защиты информации в дискретном канале на основе избыточных представлений чисел // 2-я Международная конференция "Теория и техника передачи, приема и обработки информации"; тез. докл. / ХТУРЭ, Туапсе, 1996. - Часть II. с.314.

В роботах, написаних у співавторстві, особисто автором розроблено:

I. Оптимальні завадостійкі до віртуальних A_1, A_2-послідовностей алгоритми одномірного пошуку точки екстремуму унімодальної функції.

2. Завадостійкі логічно нескладні алгоритми одномірного пошуку точки екстремуму унімодальної функції.

3. Конкретні завадостійкі до A_1, A_2-послідовностей алгоритми одномірного пошуку.

4. Співвідношення для вирішуючої функції пошуку, які дозволяють виділити новий інтервал невизначеності і розподілити точки наступного експерименту.

5. Генератори псевдовипадкових ключів для методу підстановок, які дозволяють псевдовипадковим чином змінити довжину ключа і його значення.

6. Надлишкові зображення десяткових чисел, на основі яких синтезуються методи захисту інформації від несанкціонованого доступу і від випадкових завад, які діють у дискретному каналі передачі інформації.

7. Структурні схеми кодуючих і декодуючих пристроїв дискретного каналу передачі інформації для методів захисту інформації, синтезованих на основі завадостійких алгоритмів.

АННОТАЦИЯ

Алипов И.Н. И. Методы защиты информации при ее передаче. Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.08 - Вычислительные машины, системы и сети, элементы и устройства вычислительной техники и систем управления, Харьковский государственный технический университет радиоэлектроники, Харьков, 1997. Предложены на основе дискретных автоматов с псевдослучайными переходами из одного состояния в другое новые методы защиты информации, обладающие высокой эффективностью. Функционирование таких автоматов описывается синтезированными в работе помехоустойчивыми к виртуальным помехам алгоритмами поиска точки экстремума унимодальной функции. Это приводит к тому, что каждой букве входного алфавита соответствует некоторое подмножество кодовых комбинаций, имеющих различную длину. Выбор кодовых комбинаций осуществляется псевдослучайным образом. Для раскрытия шифротекста необходимо знать параметры виртуальной помехи, алгоритм ее формирования, вид унимодальной функции и логическую схему помехоустойчивого алгоритма.

THE SUMMARY

Alipov I.N. The information protection methods at its transmission. Dissertation for candidate degree of technical sciences on speciality 05.13.08 - computers, complexes and networks, units and devices of computers and control systems. Kharkov State technical University of Radioelectronics. Kharkov, 1997. The new informations protection methods having high efficiency are offerred on the basis of discrete automatic devices with pseudorandom branches from one state in other. The functioning of such automatic devices is described by unimodal function extremum point hunt algorithms synthesized in the work, which are noiseimmunity to virtual noises. It results in that, that to each letter of source alphabet corresponding some subset of code combinations, having various length. The choosing of code combinations is realized by pseudorandom mode. To unravel a cipher text it is necessary to know the parameters of virtual handicapes, algorithm its formation, unimodal functions kind and logic outline of noiseimmunity algorithm.

Ключові слова: алгоритм, пошук, завадостійкість, оптимальність, зображення десяткових чисел, кодування, віртуальна завада, унімодальна функція, надлишковість, точка екстремуму унімодальної функції, стратегія пошуку, вирішуюча функція, автомат із псевдовипадковими переходами.

Підп. до друку 12.06.97. Формат 60x84 1/16. Папір друк. Друк офсетний.
Умов. друк. арк. 1,1. Облік вид. арк. 1,0. Тираж 100 прим.

Надруковано у видавництві ХТУРЕ.

310726 Україна Харків, просп. Леніна, 14.