



УКРАЇНА

(19) **UA** (11) **145773** (13) **U**
(51) МПК

H03M 7/40 (2006.01)

H03M 13/01 (2006.01)

H03M 13/07 (2006.01)

НАЦІОНАЛЬНИЙ ОРГАН
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
ДЕРЖАВНЕ ПІДПРИЄМСТВО
"УКРАЇНСЬКИЙ ІНСТИТУТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2020 02967**
(22) Дата подання заявки: **18.05.2020**
(24) Дата, з якої є чинними
права інтелектуальної
власності: **07.01.2021**
(46) Публікація відомостей
про державну
реєстрацію: **06.01.2021, Бюл.№ 1**

(72) Винахідник(и):
**Бараннік Володимир Вікторович (UA),
Бараннік Валерій Володимирович (UA),
Стеценко Оксана Миколаївна (UA),
Рябуха Юрій Миколайович (UA),
Пархоменко Максим Вікторович (UA),
Тупиця Іван Михайлович (UA),
Малько Олександр Дмитрович (UA),
Коломійцев Олексій Володимирович
(UA),
Пугачов Роман Володимирович (UA),
Мусієнко Олександр Павлович (UA)**

(73) Володілець (володільці):
**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ ПОВІТРЯНИХ СИЛ ІМЕНІ
ІВАНА КОЖЕДУБА,
вул. Сумська, 77/79, м. Харків, 61023 (UA)**

(54) СПОСІБ ВНУТРІШНЬОЇ РЕСТРУКТУРИЗАЦІЇ ДАНИХ ДЛЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО РЕСУРСУ

(57) Реферат:

Спосіб внутрішньої реструктуризації даних для безпеки інформаційного ресурсу. Змінюють потужність алфавіту повідомлення в телекомунікаційних мережах за рахунок кластеризації елементів повідомлення за кількісною ознакою (ознакою кількості серій одиниць), а статистичне кодування елементів проводять в межах множин, які утворюють.

UA 145773 U

UA 145773 U

Корисна модель належить до галузі телекомунікаційних технологій і може бути використана в сучасних інформаційно-телекомунікаційних системах та мережах.

Відомий "Спосіб ентропійного кодування на основі коду Хаффмана" [1], в якому зіставляються кожному елементу вхідної послідовності різне число елементів вихідної послідовності на основі побудови кодів змінної довжини з метою зменшення об'єму даних.

Недоліком відомого способу є те, що даний спосіб не дозволяє забезпечити захист даних в разі несанкціонованого доступу.

В основу корисної моделі поставлена задача створити спосіб внутрішньої реструктуризації даних для безпеки інформаційного ресурсу, який дозволить враховувати закономірності у внутрішній структурі елементів повідомлення та забезпечить надійний рівень безпеки інформаційного ресурсу.

Поставлена задача вирішується спосіб внутрішньої реструктуризації даних для безпеки інформаційного ресурсу. Змінюють потужність алфавіту повідомлення в телекомунікаційних мережах за рахунок кластеризації елементів повідомлення за кількісною ознакою (ознакою кількості серій одиниць), а статистичне кодування елементів проводять в межах множин, які утворюють.

Технічний результат, який може бути отриманий при здійсненні корисної моделі полягає у підвищенні ефективності статистичного кодування даних інформаційного ресурсу з позиції скорочення довжини на представлення інформації на 12 % та безпеки даних інформаційного ресурсу.

Запропонований спосіб внутрішньої реструктуризації даних для безпеки інформаційного ресурсу, який змінює потужність алфавіту повідомлення в телекомунікаційних мережах за рахунок кластеризації елементів повідомлення за кількісною ознакою (ознакою кількості серій одиниць), а статистичне кодування елементів відбувається в межах множин, які утворюються.

Робота запропонованого способу внутрішньої реструктуризації даних для безпеки інформаційного ресурсу полягає у наступному [2].

Внутрішня реструктуризація здійснюється за рахунок виявлення закономірностей у внутрішній структурі елементів повідомлення $U(\theta)$ за кількісною ознакою λ_i . Кількість різних значень, які приймає ознака (потужність ознаки) λ_i , може бути n . Набір різних значень ознаки λ_i описується наступним виразом:

$$\Lambda = \{\lambda_1, \dots, \lambda_i, \dots, \lambda_n\}, \quad (1)$$

де Λ - набір значень ознаки λ_i , що виявлено у внутрішній структурі елементів u_ξ повідомлення $U(\theta)$, λ_i, λ_n - значення i -ї і n -ї ознаки набору Λ .

Як внутрішня структура елемента u_ξ повідомлення $U(\theta)$ використовується його двійкове подання. Елемент u_ξ повідомлення $U(\theta)$ складається з послідовності $[u_\xi]_2$ двійкових розрядів $q_{\xi, \alpha}$.

$$[u_\xi]_2 = \{q_{\xi, 1}; \dots; q_{\xi, \alpha}; \dots; q_{\xi, |u_\xi|_2}\}, \quad (2)$$

де $[u_\xi]_2$ - двійкове подання елемента u_ξ повідомлення $U(\theta)$, $q_{\xi, \alpha}$ - α -й розряд елемента u_ξ .

Кількість різних комбінацій η , які приймає окремий елемент u_ξ повідомлення $U(\theta)$, задається наступним виразом:

$$\eta = 2^{|u_\xi|_2}, \quad (3)$$

де η - кількість комбінацій значень, які може приймати елемент u_ξ , $|u_\xi|_2$ - довжина елемента u_ξ (кількість розрядів $q_{\xi, \alpha}$, якими представляється елемент u_ξ).

Далі проводиться кластеризація (групування) елементів u_ξ повідомлення $U(\theta)$ за значенням кількісної ознаки λ_i , яка визначає закономірності у внутрішній структурі елементів u_ξ повідомлення $U(\theta)$.

Кластеризація за кількісною ознакою полягає у тому, що елементи u_ξ повідомлення $U(\theta)$ з однаковими значеннями кількісної ознаки λ_i формують множини $U(\lambda_i)$:

$$U(\theta) \xrightarrow{f_{cl}} \{U(\lambda_1), \dots, U(\lambda_i), \dots, U(\lambda_n)\}, \quad (4)$$

де f_{cl} - функція групування елементів u_ξ у множини $U(\lambda_i)$ за значенням ознаки λ_i , n - кількість множин $U(\lambda_i)$, які формуються в процесі кластеризації елементів u_ξ повідомлення $U(\theta)$.

5 Кількість множин $U(\lambda_i)$, які формуються в процесі кластеризації, визначається набором Λ значень ознаки λ_i . До кластеризації елементів u_ξ повідомлення $U(\theta)$ за кількісною ознакою λ_i ставляться наступні вимоги:

- повідомлення $U(\theta)$ розбивається на множини $U(\lambda_i)$ таким чином, щоб кожен елемент u_ξ повідомлення $U(\theta)$ належав одній і тільки одній множині розбиття, тобто множини не

10 перетинаються, якщо $u_\xi \in U(\lambda_i)$, то $u_\xi \notin U(\lambda_j)$, де $i \neq j$, $\lambda_i, \lambda_j \in \Lambda$, та $U(\lambda_j) \cap U(\lambda_i) = \emptyset$;

- елементи u_i і u_ξ , які належать одній і тій самій множині $U(\lambda_i)$, мають однакові значення ознаки λ_i , тобто:

якщо $u_i \in U(\lambda_i)$, $u_\xi \in U(\lambda_i)$, то $\lambda_i(u_i) = \lambda_i(u_\xi)$;

15 - елементи u_i і u_ξ , що належать різним множинам повинні мати значення ознаки λ_i , тобто: якщо $u_i \in U(\lambda_j)$, $u_\xi \in U(\lambda_i)$, то $\lambda_j(u_i) \neq \lambda_i(u_\xi)$;

- сума довжин множин (кількість елементів у множині) $U(\lambda_i)$ (де $i = \overline{1, n}$), утворених в процесі кластеризації дорівнює довжині $|U(\theta)|$ вхідного повідомлення $U(\theta)$, тобто:

$$|U(\theta)| = \sum_{i=1}^n |U(\lambda_i)|,$$

20 де $|U(\lambda_i)|$ - довжина множини $U(\lambda_i)$, $|U(\theta)|$ - довжина вхідного повідомлення $U(\theta)$, n - кількість множин $U(\lambda_i)$.

Елементи u_ξ , які мають однакові значення ознаки λ_i , кодуються в межах сформованих множин $U(\lambda_i)$. Проводиться статистичне кодування елементів u_ξ множини $U(\lambda_i)$, які складаються з κ - елементів (тобто $\xi = \overline{1, \kappa}$) задається наступним співвідношенням:

25 $U(\lambda_i) \xrightarrow{f_{vlc}} L(\kappa), \quad (5)$

де $f_{vlc}(u_\xi, P_{сл})$ - функція формування статистичного коду l'_ξ змінної довжини (variable length coding-VLC) для елементів u_ξ множини $U(\lambda_i)$, $P_{сл}$ - службова інформація про розподіл значень ймовірностей появи елементів u_ξ в множині $U(\lambda_i)$.

На основі функції $f_{vlc}(u_\xi, P_{сл})$ формується код l'_ξ :

30 $l'_\xi = f_{vlc}(u_\xi, P_{сл}). \quad (6)$

В результаті статистичного кодування елементів u_ξ множини $U(\lambda_i)$ утворюється послідовність $L(\kappa)$ кодів l'_ξ ;

$$L(\kappa) = \{l'_1; \dots; l'_\xi; \dots; l'_\kappa\}, \quad (7)$$

де κ - кількість елементів в послідовності кодів $L(\kappa)$

35 Код l'_ξ є кодом змінної довжини $|l'_\xi|_2, |l'_\xi|_2 = \text{VAR}$, і складається з послідовності $|l'_\xi|_2$

двійкових розрядів $q_{\xi, \gamma}$, $\gamma = 1, |l'_\xi|_2$:

$$|l'_\xi|_2 = \{q_{\xi, 1}; \dots; q_{\xi, \gamma}; \dots; q_{\xi, |l'_\xi|_2}\}, \quad (8)$$

де $q_{\xi, \gamma}$ - γ -й розряд коду l'_ξ .

Використання кластеризації знижує потужність $|U(\theta)|$ алфавіту на базі якого формуються елементи u_ξ повідомлення $U(\theta)$, тобто:
 $|U(\lambda_i)| < |U(\theta)|$.

5 Статистичне кодування елементів u_ξ повідомлення $U(\theta)$ в межах сформованих множин $U(\lambda_i)$ утворює кодові конструкції ℓ'_ξ , які мають властивість міжмножинної префіксності. Тобто, властивість префіксності дотримується тільки для кодів ℓ'_ξ елементів u_ξ , які належать одній множині $U(\lambda_i)$. Якщо елементи u_i і u_j належать одній і тій самій множині $U(\lambda_i)$, то код ℓ'_i довжиною $|\ell'_i|_2$, який присвоюється елементу u_i , не є початковою частиною іншого коду ℓ'_j довжиною $|\ell'_j|_2$, який присвоюється елементу u_j .

10 При статистичному кодуванні елементів u_ξ множин $U(\lambda_i)$ можливі наступні варіанти розвитку подій:

1) існує ймовірність того, що різним за значенням елементам u_ξ і u_j , які належать різним множинам, можуть присвоюватися однакові коди, тобто:
 якщо $u_\xi \in U(\lambda_i)$, $u_j \in U(\lambda_j)$, то $\ell'_\xi = \ell'_j$.

15 2) однозначне декодування кодових конструкцій ℓ'_ξ , які присвоюються елементам u_ξ множин $U(\lambda_i)$, буде можливим тільки при наявності інформації, якій з множин $U(\lambda_i)$ належить той чи інший елемент повідомлення $U(\theta)$.

Джерела інформації:

20 1. Кормен Томас Х. Алгоритмы: Построение и анализ. Introduction to Algorithms. - 2-е изд. / Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн. - М.: Вильямс, 2006. - 1296 с.

2. Тупиця І.М. Методологія реструктуризації даних інформаційного ресурсу для підвищення ефективності статистичного кодування / І.М. Тупиця // Наукоємні технології: - 2019. - № 2(52). - С. 262-269.

25

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

30 Спосіб внутрішньої реструктуризації даних для безпеки інформаційного ресурсу, який **відрізняється** тим, що змінюють потужність алфавіту повідомлення в телекомунікаційних мережах за рахунок кластеризації елементів повідомлення за кількісною ознакою (ознакою кількості серій одиниць), а статистичне кодування елементів проводять в межах множин, які утворюють.