УДК 621.39

ОБҐРУНТУВАННЯ ПІДХОДУ ЩОДО СТВОРЕННЯ ТЕХНОЛОГІЇ КІБЕРЗАХИСТУ ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ В ІНФОКОМУНІКАЦІЙНОМУ ПРОСТОРІ

В. В. Бараннік, д-р техн. наук, проф., ***С. А. Підлісний***

Харківський університет Повітряних Сил імені Івана Кожедуба

Barannik_V_V@mail.ru

Розглянуто технологію розміщення кодів змінної довжини в слоті однакової довжини за сучасних загрозах в інформаційно-телекомунікаційних системах. Відображено вплив викривлення прийнятих кодів змінної довжини на цілісність відеоінформаційного ресурсу. Розглянуто процес відновлення елементів зображення за наявності помилки в прийнятому слоті. Обґрунтовано умови для ефективного кодування під час застосування технології слотування кодів змінної довжини.

Ключові слова: інформаційна безпека, відеоінформаційний ресурс, інформаційна інтенсивність, кібератака.

Consider the placing technology of variable length codes in the slots of equal length with modern threats in information and telecommunication systems. Displaying effect distortion variable length codes adopted by the integrity of video information resource. The process of restoration of picture elements if errors in accepted slot. Substantiated conditions for efficient coding in using of slots technology of variable length codes.

Keywords: information security, video information resource, information intensity, cyberattack.

Вступ

На сьогодні широкого застосування набула передача відеоінформаційного ресурсу в одному напрямку в системах відеомоніторингу та двоспрямована передача в системах відеозв'язку. Ці системи розповсюджені у державних відомчих установах, особливо в Міністерстві оборони України. Використання відеоінформаційного ресурсу призводить до поліпшення якості системи управління [1].

У зв'язку з важливістю змісту відеоінформаційний ресурс потребує захисту. Це пов'язано зі зростанням кібернетичних загроз державним установам, що виникають в результаті здійснення кібератак [2].

Одним з найпоширеніших видов кібератак є атаки типу DDoS-атака [3]. Це зумовлюється насамперед легкістю реалізації даного типу атаки. Існуючі методи кіберзахисту, що працюють на різних мережевих рівнях [4], виявляють кібератаку за відповідністю кількісним параметрам. Це призводить до реакції лише при настанні активної фази атаки, коли вона вже виявлена.

Характер впливу кібератак на відеоінформаційний ресурс пов'язаний з особливістю його обробки. У сучасних методів обробки (JPEG, MPEG-4, H.264) застосовується стискання на базі статистичного кодування (кодів змінної довжини). Дане кодування є ефективним щодо забезпечення високого ступеня стиснення за достатньої якості відновлення зображення [5]. При даному кодуванні опорні кадри відео- передаються протягом невеликого проміжку часу відносно тривалості усієї послідовності кадрів. При цьому на бітові складові кодів змінної довжини опорних кадрів можуть впливати викривлення, що виникають природним або штучним шляхом [6] (використання різноманітних кібернетичних атак). За умови здійснення зазначених кібератак результатом викривлення невеликої ділянки закодованих даних буде втрата значної частини потоку відеоінформаційного ресурсу, унаслідок цього порушуються такі характеристики інформаційної безпеки ресурсу, як цілісність та доступність. На виявлення кібератак існуючим системам кіберзахисту потрібен деякий час, що призводить до ситуації, коли за наявності короткотривалих атак це призводить до унеможливлення реакції. Для динамічних умов відеоінформаційного ресурсу даний тип реакції вважається не припустимим.

З цього випливає проблема недостатнього рівня оперативної протидії кіберзагрозам для існуючих методів захисту. Для вирішення проблеми локалізації дії кібератак необхідно обґрунтувати та розробити відповідний метод обробки відеоінформаційного ресурсу. Для цього потрібно виявити недоліки існуючих технологій кодування відеоданих з метою їх усунення. На цієї базі необхідно проаналізувати вплив викривлення бітових складових кодів змінної довжини на процес відновлення вихідного відеоінформаційного ресурсу. Отже, потрібно розробити таку технологію, яка локалізує дію бітових помилок на відеоінформаційний ресурс.

Мета роботи — обґрунтувати підхід щодо створення технології кіберзахисту відеоінформаційного ресурсу в інфокомунікаційному просторі.

Основна частина

Розглянемо існуючу схему обробки відеоданих за допомогою статистичного кодування.

Статистичному кодуванню підлягають компоненти u_ξ лінеаризованої трансформанти, що утворились після дискретно-косинусного перетворення сегментів вихідного зображення. Кодування задається таким відношенням:

$$U(\theta) \xrightarrow{f_{vlc}} L(\theta),$$

де $f_{vlc}(u_\xi, P_{сл})$ — функція формування статистичного коду ℓ_ξ змінної довжини (variable length coding — VLC) для компонент u_ξ вектора $U(\theta)$ [7].

Коду змінної довжини властива префіксність. Унаслідок використання символів-розподілювачів для визначення початкового розряду $q_{\xi,1}$ кожного коду ℓ_ξ під час побудові елементів послідовності не потрібно. Це визначає можливість однозначного декодування кожного коду. Декодування при цьому відбувається послідовно, тобто декодер приступає до декодування наступного коду $\ell_{\xi+1}$ лише після однозначного декодування коду ℓ_ξ та визначення його довжини.

Розглянемо вплив помилки у VLC кодах на процес статистичного декодування компоненти u_ξ лінеаризованої трансформанти.

Умовно приймемо, що помилка відбулась у 2-му розряді коду ℓ_5 с утворенням коду ℓ_5^* (рис. 1).

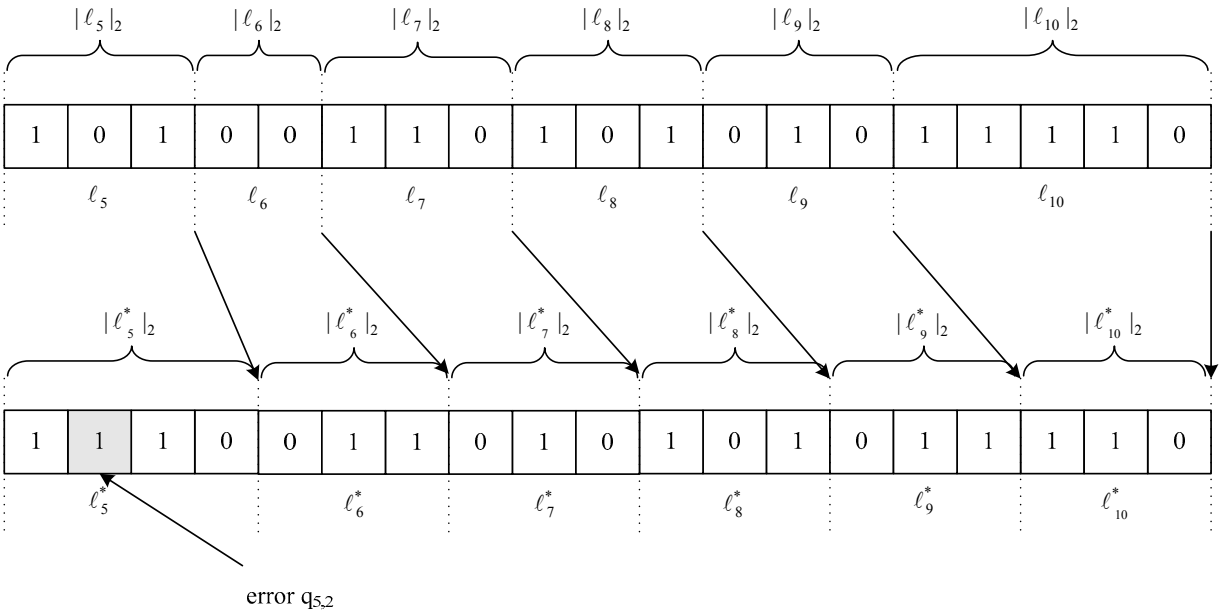

Рис. 1. Вплив бітової помилки на процес декодування кодів змінної довжини

За наявності бітової помилки у коді ℓ_5 відбувається невірна ідентифікація коду ℓ_5^* та його довжини $|\ell_5^*|_2$, що призводить до подальшій невірній ідентифікації всіх наступних VLC кодів.

Це аргументується тим, що за наявності бітової помилки в потоці кодів змінної довжини вплив помилки може дуже впливати на відновлення значень коефіцієнтів ДКП [8], тобто статистичний код не є стійким до помилок.

Для зменшення впливу бітової помилки використовують технологію стійкого до помилок ентропійного кодування (EREC) [7].

Це визначається так:

$$L(\theta) \xrightarrow{f_{erec}} S(\Lambda),$$

де f_{erec} — функція розподілу VLC кодів ℓ_ξ змінної довжини в слоті s_λ; Λ — кількість слотів, в які розподілені VLC коди.

Технологія EREC характеризується наступними етапами розміщення і подальшого перерозподілу вмісту кодових конструкцій ℓ_ξ.

Дана технологія розміщує VLC коди ℓ_ξ в слоті пакету EREC $S(\Lambda)$ на основі перебудови бітової структури. Тут враховується, що слотами є кодові слова рівномірної довжини, тобто:

$$|s_i|_2 = |s_j|_2 = \upsilon, \text{ при } i \neq j$$

Пакет, перетворений технологією EREC, складається з Λ слотів s_λ довжина υ бітів і має загальну довжину $|S(\Lambda)|_2 = \Lambda \times \upsilon$.

Технологія EREC розміщує коди ℓ_ξ VLC в послідовності довжиною $|\ell_\xi|_2$ у пакет EREC слоту $S(\Lambda)$ шляхом перебудови розрядної структури, що призводить до можливості визначення кінця кожного коду.

Довжина υ слота s_λ залежить від відношення загальної довжини $|L(\theta)|_2$ послідовності L(θ) кодів до кількості слотів Λ:

$$\upsilon = \frac{|L(\theta)|_2}{\Lambda} = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\theta} |\ell_i|_2 \right\rceil,$$

де [x] — оператор округлення значення x до більшого натурального числа.

Після того, як визначилось значення довжини $|S(\Lambda)|_2$ пакета EREC, отримуємо

$$|S(\Lambda)|_2 = \upsilon \times \Lambda,$$

тобто відбувається впорядковування коду згідно з наступним алгоритмом.

У першій стадії алгоритм кожного коду розміщується ℓ_ξ у відповідному EREC слоті s_ξ.

На наступних етапах надлишкові частини кожного коду поділяються по залишках слотів.

Схематичний результат розподілу всієї послідовності VLC кодів у пакет слотів, відповідно до технології EREC, показано на рис. 2.

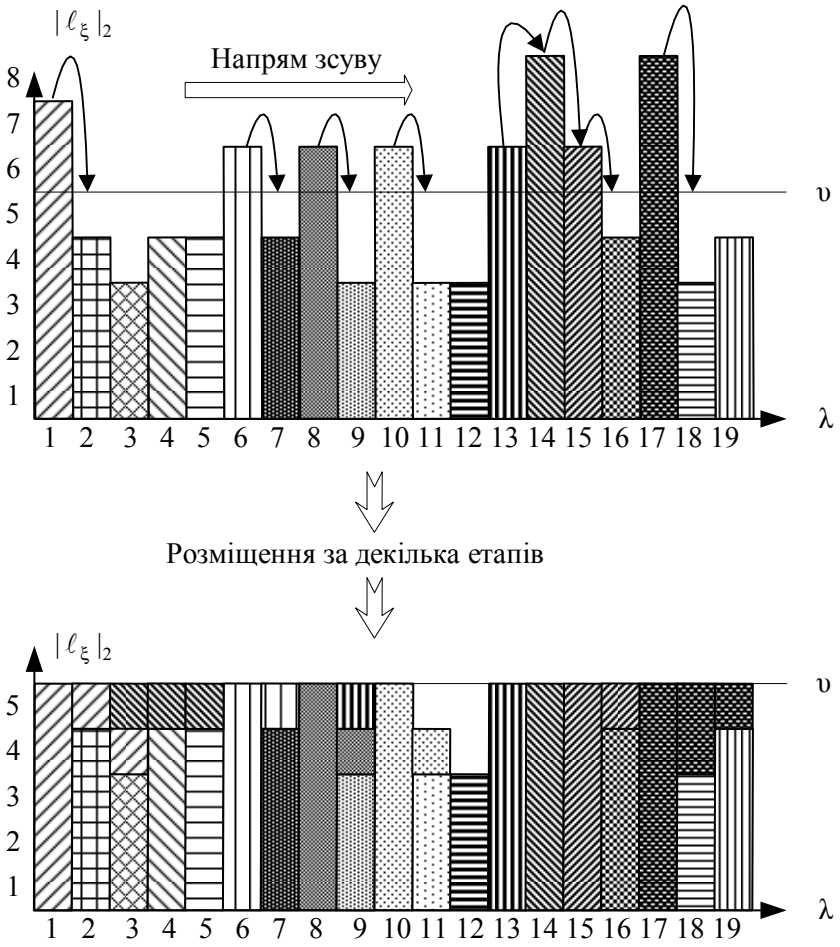

Рис. 2. Результат розміщення базових складових кодових конструкцій у сформованому пакеті слотів

Після розміщення VLC кодів ℓ_ξ у пакеті слотів $S(\Lambda)$ відбувається відправлення пакету слотів $S(\Lambda)$ та його довжини $|S(\Lambda)|_2$.

Залишкову надмірність δ застосованої технології знаходять як різницю між довжиною $|S(\Lambda)|_2$ пакета слотів і довжиною $|L(\theta)|_2$ послідовності кодів:

$$\delta = \sum_{i=1}^{\Lambda} \upsilon - \sum_{i=1}^{\theta} |\ell_i|_2$$

У зв'язку з цілим значенням довжини υ слоту 3, максимальна кількість надлишкових біт залежить від кількості слотів:

$$\delta_{\max} = \Lambda - 1$$

У процесі реструктуризації VLC кодів, за відсутності помилок у каналі, згідно з цим алгоритмом відбувається ідентифікація коду змінної довжини для кожного VLC коду ℓ_ξ з відновленням значення лінеаризованої трансформанти u_ξ.

При цьому використовують існуючий механізм декодування статистичних кодів.

Зазначена властивість технології щодо ідентифікації початку кожного VLC коду ℓ_ξ дає можливість проводити паралельну ідентифікацію всіх компонент u_ξ лінеаризованої трансформанти.

Разом з цим слід зазначити, що перехід на наступний етап реструктуризації VLC кодів відбувається лише після завершення поточного етапу для всіх VLC кодів. Тобто надається можливість підвищення оперативності доведення відеоданих при внесенні надмірності у послідовність кодів.

Алгоритм зворотної реструктуризації триває до заключної ідентифікації всіх компонент лінеаризованої трансформанти. Вплив помилки на процес декодування залежить від того, який розділ слота був пошкоджений і як були розподілені дані по слотах. Наприклад, помилка в слоті 1 призводить до невірного визначення цього коду і подальшої помилки в ідентифікації деяких кодів.

Результат неправильного визначення довжини коду для даного випадку показано на рис. 3.

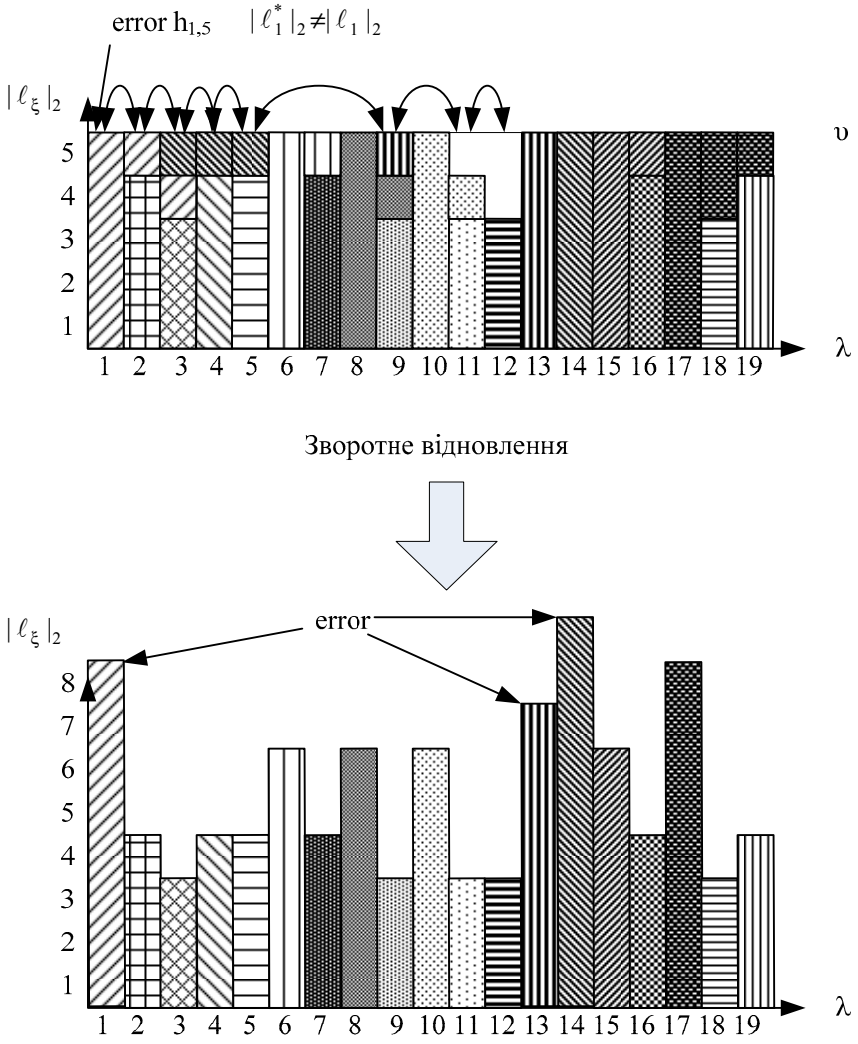

Рис. 3. Вплив помилки в 5-му біті 1-го слота на визначення довжин усіх кодів

У разі неправильного декодування першого коду ℓ_1, декодер неправильно визначає довжину $|\ell_1|_2$ першого коду. Для зворотної реструктуризації коди з 2 на 12 і з 15 на 19 залишаться без змін. Для кодів 1, 13 і 14 декодер може використовувати і попереднє і наступне значення бітів, визначених алгоритмом реструктуризації.

У результаті помилка в першому слоті призведе до неправильного декодування коду з індексом 1, 13 і 14. За відсутності розподілу кодів по слотах помилка може поширитися на усі кодовані блоки.

З вищенаведеного випливає, що використання технології пружного до помилок ентропійного кодування EREC краще забезпечує доступність та цілісність відеоінформаційного ресурсу порівняно з існуючим статистичним кодуванням. При цьому це досягається незначною залишковою надмірністю.

Висновки

1. Обґрунтовано, що застосування існуючих механізмів обробки інформації з використанням статистичного кодування за умови здійснення кібернетичних атак призводить до порушення цілісності та доступності відеоінформаційного ресурсу.

2. Для виявлених уразливостей для локалізації розповсюдження помилки в статистичному коді пропонується розподіл кодів змінної довжини в однакові за довжиною кодові конструкції (слоти).

3. Обґрунтовано підхід щодо створення технології кіберзахисту відеоінформаційного ресурсу в інфокомунікаційному просторі та розроблення технології, що локалізує порушення інформаційної безпеки відеоінформаційного ресурсу в умовах дії кібератак, що базується на технології слотування для VLC кодів.

ЛІТЕРАТУРА

1. *Аналіз* дії кібератак на відеоінформаційний ресурс в інформаційно-телекомунікаційних мережах / В. В. Бараннік, С. А. Підлісний // АСУ та прилади автоматики: науково-технічний збірник. — Вип. 164. — Х. : ХНУРЕ. — 2014. — С. 16–22.

2. *Захист* інформаційних мереж є питанням державної безпеки — голова Держспецзв'язку Геннадій Резніков. — [Електронний ресурс] http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712, 2015.

3. *Звіт* CERT-UA за 2014 рік, [Електронний ресурс], http://cert.gov.ua/?p=2019, 2015.

4. *Мартынюк И*. Материалы технического тренинга «Построение безопасных сетей на оборудовании D-Link», [Електронний ресурс], http://service.d-link.ua/sites/default/files/files/Security.zip. — К., 2012. 190 с.

5. *Richardson E*. "H.264 and MPEG-4 video compression,". — Chichester, UK: Wiley and Sons, 2003. — 306 p.

6. *Wang Y*. "Error control and concealment for videocommunication: A review," / Y. Wang, Q. F. Zhu. Proceedings of the IEEE, vol. 86, no. 5. — P. 974–997, May 1998.

7. *Gonzales R. C*. "Digital image processing," in Prentice Hall, edition. II / R. C. Gonzales, R. E. Woods, 2002. — 1072 p.

8. *Mohammed E*. "Video coding for mobile communications / E. Mohammed, C. Canagarajah and D. Bull // Efficiency, complexity snd resilience," Elsevier Science, 2002. — 283 p.

9. *Dogan S*. "Error-resilient techniques for video transmission over wireless channels," Arabian journal for science and engineering / S. Dogan, A. H. Sadka and A. M. Kondoz, 1999. — P. 101–114.

Стаття надійшла до редакції 29.02.2016