

# КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ И ТЕХНИЧЕСКАЯ ДИАГНОСТИКА



УДК 621.39

## МЕТОД ЛОКАЛИЗАЦИИ ПОТЕРИ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ СЛОТ-ТЕХНОЛОГИИ

*БАРАННИК В.В., ПОДЛЕСНЫЙ С.А.,  
БАРАННИК Д.В.*

Показывается проблематичность обеспечения информационной безопасности государственного видеoinформационного ресурса. Рассматриваются основные недостатки статистического кодирования при обработке видео в случае применения кибератак. Обосновывается необходимость разработки технологии распределения кодов переменной длины для видеопотока. В результате этого формируется механизм локализации потери целостности информации.

**Ключевые слова:** видеoinформационный ресурс, кибератака, обработка видео, информационная безопасность.

**Keywords:** video information resource, cyber attack, video processing, information security.

### 1. Введение

В результате бурного развития информационных технологий появилась возможность применения видеoinформационного ресурса в государственных учреждениях. Итогом данного нововведения явилось улучшение качества системы управления [1]. Использование видеoinформационного ресурса для односторонней передачи реализовано в системах видеомониторинга, а для двунаправленной – в системах видеосвязи. В связи с важностью содержания видеoinформационный ресурс, как и любой другой государственный информационный ресурс, нуждается в защите [2]. Это обусловлено ростом кибернетических угроз государственным учреждениям, возникающих в результате кибератак [3].

В связи с легкостью осуществления наиболее распространенными видами кибератак являются атаки типа DDoS [4]. Существующие механизмы киберзащиты, работающие на различных сетевых уровнях [5], идентифицируют кибератаку по соответствию количественных параметров. Результатом данного типа реакции является обнаружение атаки, когда она уже перешла в активную фазу. Кибератака проявляется внешне как искажение, пропадание и полная недоступность видеoinформационного ресурса.

Вследствие этого наступает необходимость улучшения информационной безопасности видеoinформационного

ресурса путем разработки технологии кодирования с учетом воздействия кибератак на ресурс. Актуальность работы связана с важностью видеoinформационного ресурса и необходимостью увеличения его устойчивости к нарушениям информационной безопасности.

Для решения поставленной задачи необходимо рассмотреть существующие технологии обработки видеoinформационного ресурса. Существующие технологии (JPEG, MPEG-4, H.264) применяют сжатие на основе статистического кодирования (кодов переменной длины) [6]. Уменьшение информационной интенсивности связано с наличием корреляционной связи между кадрами в группе кадров. Данная группа кадров состоит из опорного кадра и последовательности разностных и обратных кадров. При этом на объем опорного кадра видео приходится малая доля объема всей группы кадров. Применение опорных кадров в процессе обработки приводит к уменьшению информационной интенсивности потока и в то же время повышает риск нарушения целостности и доступности потока к искажениям [7]. Это связано с возможностью потери содержимого всей группы кадров для потока видеoinформационного ресурса при искажении указанными кибератаками небольшого участка опорного кадра. В результате запаздывания реакции применение краткосрочных атак (медленной DDoS-атак) приводит к отсутствию идентификации угрозы при фактической недоступности видеoinформационного ресурса. В силу динамических условий использования видеoinформационного ресурса это считается недопустимым, так как указывает на недостаточную оперативность противодействия киберугрозам для существующих методов защиты. Это приводит к необходимости разработки технологии, которая локализует действие битовых ошибок на видеoinформационный ресурс.

Для этого необходимо рассмотреть недостатки современных технологий кодирования видеоданных. В существующей схеме обработки видеoinформационного ресурса после дискретно-косинусного преобразования сегментов исходного изображения используется статистическое кодирование полученных компонент линеаризованной трансформанты. Ввиду префиксности статистического кода переменной длины устраняется необходимость в символах-разделителях для декодирования компонент трансформанты изображения. В результате этого декодирование каждого кода производится только последовательно. При наличии битовой ошибки в коде происходит неверная идентификация кода и его длины, что приводит к дальнейшей неверной идентификации всех последующих VLC-кодов, которая выражается в разрушении всего изображения. Из этого вытекает, что наличие битовой ошибки в коде приводит к уязвимости целостности информации, которая содержится в последовательности кодов.

Поэтому цель работы заключается в создании метода локализации потери целостности информации вследствие неверного позиционирования статистических кодов при наличии ошибки в потоке и рассмотрении

изменения устойчивости видеоинформационного ресурса к ошибкам для предложенной технологии.

## 2. Разработка метода локализации потери целостности информации

Для устранения неверной идентификации начала каждого кода при битовых ошибках в целях позиционирования предлагается использовать технологию упругого к ошибкам энтропийного кодирования (Error Resilient Entropy Code – EREC). Данная технология задается функцией преобразования  $f_{\text{errec}}$ . Это определяется таким соотношением:

$$L(\theta) \xrightarrow{f_{\text{errec}}} S(\Lambda). \quad (1)$$

Здесь  $f_{\text{errec}}$  – функция распределения VLC-кодов  $\ell_\xi$  по слотам  $s_\lambda$ ;  $\Lambda$  – количество слотов, в которые распределены VLC-коды.

Технология EREC характеризуется следующими этапами:

- размещение содержимого кодовых конструкций  $\ell_\xi$ ;
- перераспределение содержимого кодовых конструкций  $\ell_\xi$ .

Данная технология размещает VLC-коды  $\ell_\xi$  в слоты пакета EREC  $S(\Lambda)$  на основе перестройки битовой структуры. Здесь учитывается, что слотами являются кодовые слова равномерной длины, т.е.:

$$|s_i|_2 = |s_j|_2 = \upsilon, \text{ при } i \neq j. \quad (2)$$

В результате преобразования последовательности  $L(\theta)$  VLC-кодов образуется пакет  $S(\Lambda)$  слотов. Вектор слотов (пакет) записывается следующим образом:

$$S(\Lambda) = \{s_1; \dots; s_\lambda; \dots; s_\Lambda\}.$$

Здесь  $s_1$  – начальный слот в пакете;  $s_\Lambda$  – последний слот в пакете.

Схематическое распределение VLC-кодов  $\ell_\xi$  по слотам  $s_\xi$ , т.е.:

$$\ell_\xi \rightarrow s_\xi^{(1)},$$

в соответствии с технологией EREC, показано на рис. 1.

В данной формуле  $s_\xi^{(1)}$  – слот, сформированный при размещении кода  $\ell_\xi$ ; (1) – индекс начального этапа, соответствующий первичному размещению VLC-кодов по слотам.

На рис. 1 представлено распределение кодового потока  $L(\theta)$ , состоящего из  $\Lambda = 19$  VLC-кодов  $\ell_\xi$  по 19 слотам. Различные VLC коды  $\ell_\xi$  представлены схематично в виде различных по окраске и размеру прямоугольников.

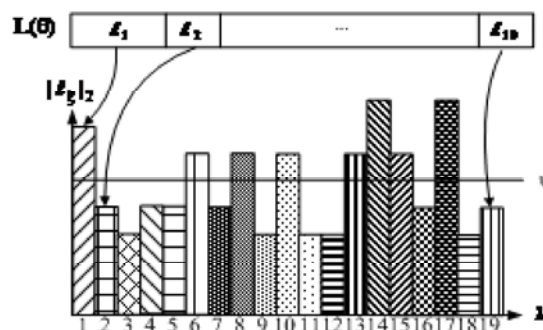


Рис. 1. Первичный этап размещения битовых составляющих кодовых конструкций при формировании пакета слотов

На первичном этапе рассматривается размещение VLC кодов  $\ell_\xi$  по слотам  $s_\xi$  без учета их выравнивания по длине  $\upsilon$ . Порядок заполнения слотов  $s_\xi$  определяется следующими правилами:

- 1) первое правило состоит в установлении порядка расстановки VLC-кодов по слотам пакета. Согласно этому правилу 1-я кодовая последовательность  $\ell_1$  размещается в слоте  $s_1$  (как показано на рис. 1);
- 2) второе правило заключается в установке порядка заполнения слотов разрядами VLC-кодов. Согласно этому правилу старшие разряды  $q_{\xi,\gamma}$ ;  $\gamma \rightarrow 1$  кодовой конструкции  $\ell_\xi$  размещаются в нижних битовых позициях слота  $s_\xi$ . Наоборот, младшие разряды  $q_{\xi,\gamma}$ ;  $\gamma \rightarrow |\ell_\xi|_2$  кодовой конструкции  $\ell_\xi$  размещаются в верхних битовых позициях слота  $s_\xi$ .

Следующим этапом формирования пакета слота является выравнивание длин кодовых слов  $s_\xi$  для выполнения условия (2) в случае, когда известно количество  $\Lambda$  слотов в пакете. Для этого сначала требуется найти длину  $\upsilon$  слота.

Длина  $\upsilon$  слота определяется как отношение суммарной длины  $|L(\theta)|_2$  последовательности  $L(\theta)$  кодов к количеству  $\Lambda$  слотов. Формула расчета длины указана в следующем выражении:

$$\upsilon = \frac{|L(\theta)|_2}{\Lambda} = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\theta} |\ell_i|_2 \right\rceil. \quad (3)$$

Здесь  $\lceil x \rceil$  – оператор округления значения  $x$  до большего натурального числа.

После определения длины  $\upsilon$  слота возможны случаи, когда длина  $|\ell_\xi|_2$  VLC-кода  $\ell_\xi$  будет превышать длину  $\upsilon$  слота

$$|\ell_\xi|_2 > \upsilon,$$

или будет меньше, т.е.:  $|\ell_\xi|_2 < \upsilon$ .

Данные случаи схематически показаны на рис. 2.

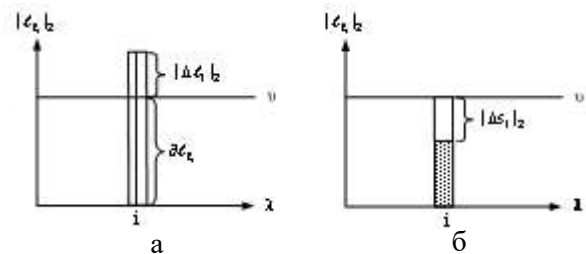


Рис. 2. Размещение VLC-кода  $\ell_i$  при заполнении слота  $s_i$  для двух случаев длины  $|\ell_i|_2$  кода  $\ell_i$ : а – длина  $|\ell_i|_2$  VLC-кода  $\ell_i$  будет превышать длину  $\upsilon$  слота; б – длина кода  $|\ell_i|_2$  VLC-кода  $\ell_i$  меньше длины  $\upsilon$  слота

Для повышения эффективности заполнения слотов в соответствии с технологией EREC происходит перераспределение избыточных составляющих  $\Delta\ell_\xi$  VLC кодов  $\ell_\xi$  по избыточным составляющим  $\Delta s_i$ ,  $i \neq \xi$  слотов  $s_i$ ,  $i \neq \xi$ , что задается формулой:

$$\Delta L(\theta) \xrightarrow{f_p} \Delta S(\Lambda), \quad (4)$$

где  $\Delta L(\theta) = \{\Delta\ell_1; \dots; \Delta\ell_\xi; \dots; \Delta\ell_\theta\}$  – совокупность избыточных составляющих  $\Delta\ell_\xi$  VLC-кодов  $\ell_\xi$ ;

$\Delta S(\Lambda) = \{\Delta s_1; \dots; \Delta s_\xi; \dots; \Delta s_\Lambda\}$  – совокупность избыточных составляющих  $\Delta s_\xi$  слота  $s_\xi$ .

Это позволит:

- 1) сохранить информацию VLC-кодов  $\ell_\xi$  на основе заполнения пустот слотов  $s_\xi$ ;
- 2) сократить избыточность, вызванную недогрузкой слота.

В общем случае избыточная составляющая  $\Delta\ell_\xi$  VLC-кода  $\ell_\xi$  будет размещена по нескольким слотам  $s_i$  (рис. 3).

Процесс перераспределения избыточных составляющих  $\Delta\ell_\xi$  VLC-кодов  $\ell_\xi$ , с учетом размещения по нескольким слотам  $s_i$ , включает в себя следующие этапы (рис. 4):

- 1) определение позиций  $i$  избыточных составляющих  $\Delta s_i$ ,

$$i = \begin{cases} \overline{\xi + 1; \Lambda} & \text{при } i > \xi; \\ \underline{1; \xi - 1} & \text{при } i < \xi \end{cases}$$

слотов  $s_i$  относительно перераспределяемой избыточной составляющей  $\Delta\ell_\xi$  кода  $\ell_\xi$ ;

- 2) определение количества  $\nu_{CM}$  и размеров  $|\Delta s_i|_2$  избыточных составляющих  $\Delta s_i$  слотов  $s_i$ , в которые будут распределены избыточные составляющие  $\Delta\ell_\xi$  для  $\xi$ -о VLC-кода. Избыточные составляющие  $\Delta s_i$  слотов  $s_i$  образуют подпоследовательность  $\Delta S(\nu_{CM})$ , которая записывается следующим образом:

$$\Delta S(\nu_{CM}) = \{\Delta s_i; \dots; \Delta s_g; \dots; \Delta s_{\nu_{CM}}\}. \quad (5)$$

Здесь  $\nu_{CM}$  – количество слотов (этапов), в которые происходит перераспределение всей избыточной составляющей  $\Delta\ell_\xi$ , длиной  $|\Delta\ell_\xi|_2$ ;  $\Delta s_g$  – избыточная составляющая слота  $s_g$  при  $g$ -м этапе заполнения слота.

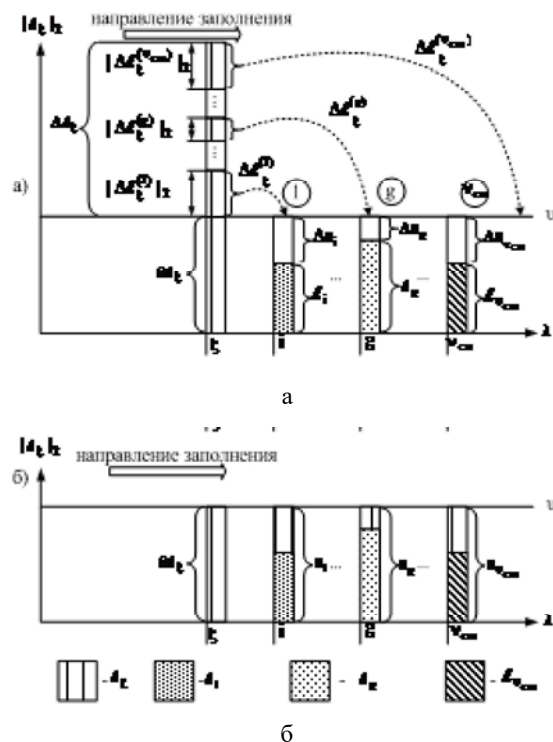


Рис. 3. Структурная схема многослотового распределения VLC: а – до распределения; б – после распределения

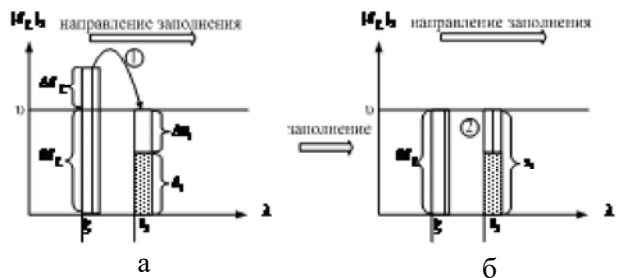


Рис. 4. Структурная схема однослотового распределения VLC: а – начало распределения; б – результат заполнения

Условие перераспределения информации без потерь заключается в обеспечении равенства суммы

$\sum_{i=1}^{v_{cm}} |\Delta s_i|_2$  размеров составляющих  $\Delta s_i$  подпоследовательности  $\Delta S(v_{cm})$  и длины  $|\Delta \ell_\xi|_2$  избыточной составляющей  $\Delta \ell_\xi$  VLC-кода  $\ell_\xi$ , т.е.:

$$\sum_{i=1}^{v_{cm}} |\Delta s_i|_2 = |\Delta \ell_\xi|_2. \quad (6)$$

Тогда для реализации процесса перераспределения избыточных составляющих  $\Delta \ell_\xi$  VLC-кодов  $\ell_\xi$  необходимо:

а) провести оценку соответствия длины  $|\Delta \ell_\xi|_2$  избыточных составляющих  $\Delta \ell_\xi$  относительно количества  $v_{cm}$  и размеров избыточных составляющих  $\Delta s_i$  слотов  $s_i$ ;

б) заполнить разрядами избыточных составляющих  $\Delta \ell_\xi$  VLC-кодов  $\ell_\xi$  позиции подпоследовательности  $\Delta S(v_{cm})$  избыточных составляющих  $\Delta s_i$  слотов  $s_i$ .

Рассмотрим механизм оценки соответствия длины  $|\Delta \ell_\xi|_2$  избыточных составляющих  $\Delta \ell_\xi$  относительно количества и размеров избыточных составляющих  $\Delta s_i$  слотов  $s_i$ . Такая оценка проводится в направлении слева направо от текущего VLC-кода  $\ell_\xi$ .

Для привязки  $i$ -й позиции к распределению составляющих  $\Delta \ell_\xi$  VLC-кодов предлагается ввести относительную нумерацию избыточных составляющих  $\Delta s_i$  слотов  $s_i$ , которые будут участвовать в распределении избыточных составляющих  $\Delta \ell_\xi$  VLC-кодов. Для этого вводится переменная  $d_g$ :

$$d_g = g - \xi,$$

значение которой определяет расстояния между позицией распределяемого VLC-кода  $\ell_\xi$  и позицией слота  $s_g$  в последовательности  $S(\Lambda)$  на  $g$ -м этапе оценки. В этом случае позиции избыточных составляющих  $\Delta s_i$  слотов  $s_i$  подпоследовательности  $\Delta S(v_{cm})$  из (5) определяются вектором  $D(v_{cm})$  смещения:

$$D(v_{cm}) = \{d_1; \dots; d_g; \dots; d_{v_{cm}}\}. \quad (7)$$

Вектор  $D(v_{cm})$  смещения характеризуется следующими свойствами:

1) количество  $v_{cm}$  элементов вектора  $D(v_{cm})$  меньше количества  $\Lambda$  слотов:  $v_{cm} < \Lambda$ ;

2) значение элемента  $d_g$  меньше количества  $\Lambda$  слотов:  $d_g < \Lambda$ ;

3) все элементы вектора  $D(v_{cm})$  различаются по величине:  $d_i \neq d_j, i \neq j$ .

В результате этого выражение (5) принимает вид:

$$\Delta S(v_{cm}) = \{\Delta s_{\xi+d_1}; \dots; \Delta s_{\xi+d_g}; \dots; \Delta s_{\xi+d_{v_{cm}}}\}.$$

При этом формула, определяющая распределение избыточной составляющей  $\Delta \ell_\xi$  VLC кода  $\ell_\xi$  по слотам, будет следующей:

$$|\Delta \ell_\xi|_2 = \sum_{g=1}^{v_{cm}} |\Delta s_{\xi+d_g}|_2, \quad d_g = \overline{1; \Lambda-1}. \quad (8)$$

Теперь рассмотрим технологию непосредственного распределения избыточной составляющей  $\Delta \ell_\xi$ , которая включает в себя следующие этапы.

На первичном этапе  $g = 1$  для избыточной составляющей  $\Delta \ell_\xi$  VLC-кода  $\ell_\xi$  с порядковым номером  $\xi$  проверяется остаток слота  $\Delta s^{(\gamma)}_{\xi+d_g}$  с позицией  $\xi + d_g$ . Данный остаток слота  $\Delta s^{(\gamma)}_{\xi+d_g}$  образовался в результате заполнения слота  $s_{\xi+d_g}$  с позицией  $\xi + d_g$  VLC-кодом  $\ell_{\xi+d_g}$  и некоторым количеством  $\gamma$  избыточных составляющих  $\Delta \ell_i$  кодов  $\ell_i$  с позицией  $i \neq \xi$  (рис. 5).

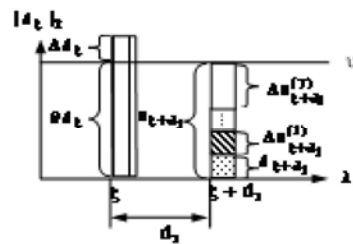


Рис. 5. Распределение VLC-кода  $\ell_\xi$  остатка слота

$$\Delta s^{(\gamma)}_{\xi+d_g}$$

Избыточная составляющая  $\Delta \ell_\xi$  распределяется в остаток слота  $\Delta s^{(\gamma)}_{\xi+d_g}$ , размер которого рассчитывается по формуле:

$$|\Delta s^{(\gamma)}_{\xi+d_g}|_2 = v - |\ell_{\xi+d_g}|_2 - \sum_{i=1}^{\gamma-1} |\Delta s^{(i)}_{\xi+d_g}|_2.$$

Избыточная составляющая слота  $\Delta s_{\xi+d_1}^{(\gamma)}$  с порядковым номером  $(\xi+d_1)$  характеризуется размером  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ . При оценке соответствия длины  $|\Delta \ell_{\xi}|_2$  избыточных составляющих  $\Delta \ell_{\xi}$  относительно размера избыточных составляющих  $\Delta s_{\xi+d_1}^{(\gamma)}$  слотов  $s_{\xi+d_1}$  возможны три результирующих варианта:

1) Длина  $|\Delta \ell_{\xi}|_2$  избыточной составляющей  $\Delta \ell_{\xi}$  равна размеру  $|\Delta s_{\xi+d_1}|_2$  избыточной составляющей  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ , т.е.:  $|\Delta \ell_{\xi}|_2 = |\Delta s_{\xi+d_1}^{(\gamma)}|_2$ .

При первом варианте оценки размера избыточная составляющая  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $s_{\xi+d_1}$  будет полностью заполнена разрядами избыточной составляющей  $\Delta \ell_{\xi}$  кода  $\ell_{\xi}$ , а именно:  $\Delta \ell_{\xi} \rightarrow \Delta s_{\xi+d_1}^{(\gamma)}$ .

При этом распределение VLC кода  $\ell_{\xi}$  по слотам заканчивается. Схематически результат заполнения показан на рис. 6.

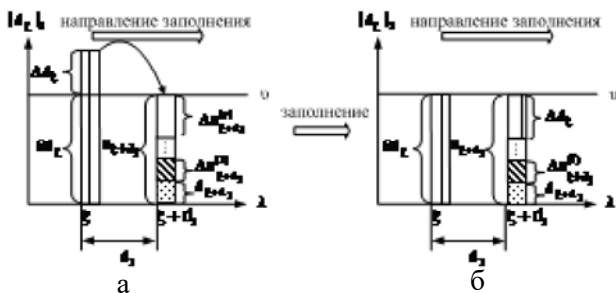


Рис. 6. Распределение VLC- кода  $\ell_{\xi}$  для условия

$|\Delta s_{\xi+d_1}|_2 = |\Delta \ell_{\xi}|_2$ : а – до распределения; б – после распределения

2) Длина  $|\Delta \ell_{\xi}|_2$  избыточной составляющей  $\Delta \ell_{\xi}$  меньше размера  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$  избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$ , т.е.:  $|\Delta \ell_{\xi}|_2 < |\Delta s_{\xi+d_1}^{(\gamma)}|_2$ .

Для данного варианта оценки соответствия длины  $|\Delta \ell_{\xi}|_2$  избыточной составляющей  $\Delta \ell_{\xi}$  относительно размера избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота

$|\Delta s_{\xi+d_1}^{(\gamma)}|_2$  изменится избыточная составляющая  $\Delta s_{\xi+d_1}^{(\gamma+1)}$  слота  $s_{\xi+d_1}$  относительно длины  $u$  слота.

Длина  $|\Delta s_{\xi+d_1}^{(\gamma+1)}|_2$  избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma+1)}$

находится как разность размера  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$  избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $s_{\xi+d_1}$  и длины  $|\Delta \ell_{\xi}|_2$  избыточной составляющей  $\Delta \ell_{\xi}$  кода  $\ell_{\xi}$ , а именно:

$$|\Delta s_{\xi}^{(\gamma+1)}|_2 = |\Delta s_{\xi+d_1}^{(\gamma)}|_2 - |\Delta \ell_{\xi}|_2.$$

При этом избыточная составляющая  $\Delta \ell_{\xi}$  кода  $\ell_{\xi}$  заполнит старшие разряды избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma+1)}$  слота  $s_{\xi+d_1}$ . Распределение VLC- кода  $\ell_{\xi}$  так же, как и для первого варианта, заканчивается. Схематически результат заполнения показан на рис. 7.

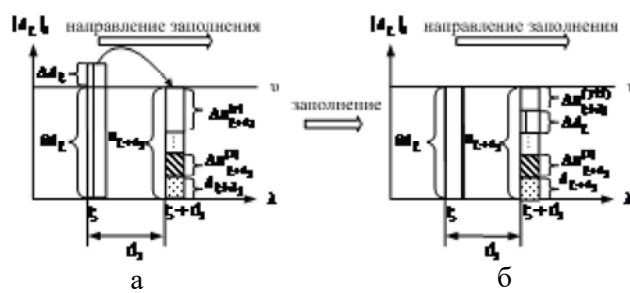


Рис. 7. Распределение VLC- кода  $\ell_{\xi}$  при

$|\Delta \ell_{\xi}|_2 < |\Delta s_{\xi+d_1}^{(\gamma)}|_2$ : а – до распределения; б – после распределения.

3) Длина  $|\Delta \ell_{\xi}|_2$  избыточной составляющей  $\Delta \ell_{\xi}$  превышает размер  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$  избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$ , т.е.:  $|\Delta \ell_{\xi}|_2 > |\Delta s_{\xi+d_1}^{(\gamma)}|_2$ .

Для данного варианта оценки соответствия длины  $|\Delta \ell_{\xi}|_2$  избыточной составляющей  $\Delta \ell_{\xi}$  относительно размера избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$  будет образована избыточная составляющая  $\Delta \ell_{\xi}^{(2)}$  кода  $\ell_{\xi}$  относительно длины избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $s_{\xi+d_1}$ .

Избыточная составляющая  $\Delta \ell_{\xi}^{(1)}$  заполнит избыточную составляющую  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $s_{\xi+d_1}$ :

$$|\Delta \ell_{\xi}^{(1)}|_2 = |\Delta s_{\xi+d_1}^{(\gamma)}|_2.$$



При этом длина избыточной составляющей  $\Delta l_{\xi}^{(2)}$  находится как разность длины  $|\Delta l_{\xi}|_2$  избыточной составляющей  $\Delta l_{\xi}$  кода  $l_{\xi}$  и размера  $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$  избыточной составляющей  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $s_{\xi+d_1}$ , а именно:  $|\Delta l_{\xi}^{(2)}|_2 = |\Delta l_{\xi}|_2 - |\Delta s_{\xi+d_1}^{(\gamma)}|_2$ .

Старшие разряды избыточной составляющей  $\Delta l_{\xi}$  кода  $l_{\xi}$  при этом заполняют избыточную составляющую  $\Delta s_{\xi+d_1}^{(\gamma)}$  слота  $s_{\xi+d_1}$ . Схематически результат заполнения показан на рис. 8.

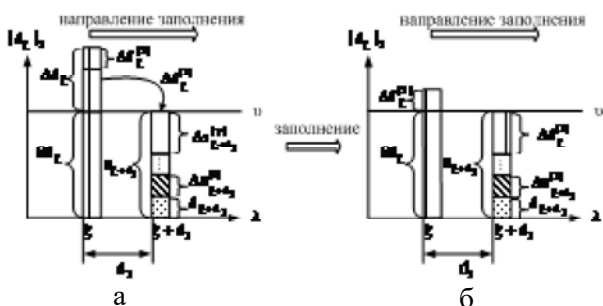


Рис. 8. Распределение VLC кода  $l_{\xi}$  при

$|\Delta l_{\xi}|_2 > |\Delta s_{\xi+d_1}^{(\gamma)}|_2$ : а – до распределения; б – после распределения

Для  $g$ -го этапа распределения избыточной составляющей  $\Delta l_{\xi}^{(g)}$  VLC-кода  $l_{\xi}$  с позицией  $\xi$  проверяется остаток слота  $\Delta s_{\xi+d_g}^{(\gamma)}$  с позицией  $\xi+d_g$ . Данный остаток слота  $\Delta s_{\xi+d_g}^{(\gamma)}$  образовался в результате заполнения слота  $s_{\xi+d_g}$  с позицией  $\xi+d_g$  VLC-кодом  $l_{\xi+d_g}$  и некоторым количеством  $\gamma$  избыточных составляющих  $\Delta l_i$  кодов  $l_i$  с позицией  $i \neq \xi$ .

Старшие разряды избыточной составляющей  $\Delta l_{\xi}$  кода  $l_{\xi}$  при этом заполняют избыточную составляющую  $\Delta s_{\xi+d_g}^{(\gamma)}$  слота  $s_{\xi+d_g}$ . Схематически результат заполнения показан на рис. 9.

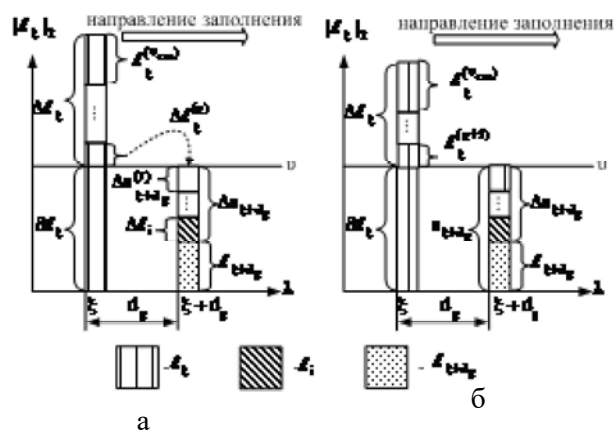


Рис. 9. Распределение VLC-кода  $l_{\xi}$  на  $g$ -м этапе: а – до распределения; б – после распределения

Этапы перераспределения VLC-кода  $l_{\xi}$  повторяются до устранения в позиции  $\xi$  положительной избыточности, вызванной перегрузкой слота.

Результат окончательного распределения VLC-кода  $l_{\xi}$  с позицией  $\xi$  за  $v_{cm}$  этапов показан на рис. 10.

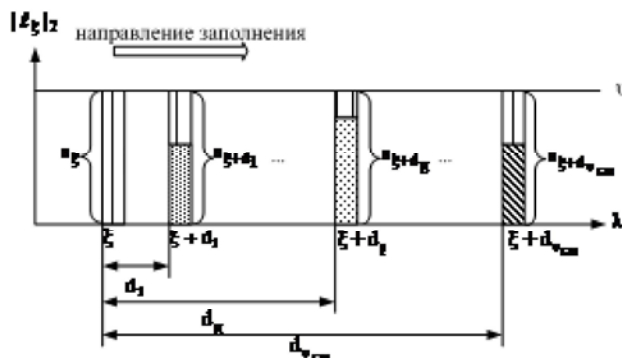


Рис. 10. Результат распределения VLC-кода  $l_{\xi}$

Различные VLC-коды  $l_{\xi}$  представлены схематично в виде различных по окраске и размеру прямоугольников.

Распределение всей последовательности  $L(\theta)$  VLC-кодов  $l_{\xi}$  происходит по аналогичному сценарию.

Остаточная избыточность  $\delta$  после перераспределения находится как разность между длиной  $|S(\Lambda)|_2$  пакета слотов и длиной  $|L(\theta)|_2$  последовательности кодов:

$$\delta = |S(\Lambda)|_2 - |L(\theta)|_2 = \Lambda \times v - \sum_{i=1}^{\Lambda} |l_i|_2. \quad (9)$$

С учетом того, что длина  $v$  слота является целым числом

$$v = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\Lambda} |\ell_i|_2 \right\rceil,$$

количество  $\delta$  остаточной избыточности определяется значением остатка от деления длины  $|L(\theta)|_2$  последовательности кодов на количество  $\Lambda$  слотов:

$$\delta \sim \left( \sum_{i=1}^{\Lambda} |\ell_i|_2 \right) \bmod \Lambda.$$

В связи с тем, что данный остаток  $\left( \sum_{i=1}^{\Lambda} |\ell_i|_2 \right) \bmod \Lambda$

имеет значения в диапазоне  $[0; \Lambda - 1]$ , количество  $\delta$  остаточной избыточности имеет следующую величину:

$$\delta \in [0; \Lambda - 1],$$

т.е. максимальное значение остаточных избыточных бит зависит от количества слотов:

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

Результат распределения всей последовательности  $L(\theta)$  VLC-кодов  $\ell_\xi$ , представленной на рис. 1, по пакету  $S(\Lambda)$  слотов  $s_\xi$ , в соответствии с технологией EREC, показан на рис. 11.

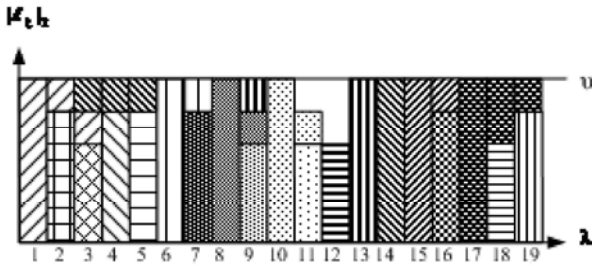


Рис. 11. Результат размещения битовых составляющих кодовых конструкций в сформированном пакете слотов

### 3. Оценка эффективности локализации битовой ошибки в последовательности кодов

Для оценки эффективности локализации битовой ошибки необходимо рассмотреть процесс декодирования распределенных VLC-кодов  $\ell_\xi$  и восстановления компонент  $u_\xi$  трансформанты на приемной стороне.

По условиям предлагаемого алгоритма необходимо идентифицировать VLC-коды  $\ell_\xi$ , полностью вошедшие в соответствующие слоты  $s_\xi$  при первичном заполнении, и определить номер  $i$ -х позиций слотов  $s_i$ , которые имеют избыточность  $|s_i|_2$ . Номер пози-

ции необходим для сборки VLC-кодов  $\ell_\xi$ , которые были распределены по нескольким слотам  $s_i$ .

В предлагаемом алгоритме количество слотов  $s_\lambda$  составляет фиксированное значение  $\Lambda$ . При этом информация о длине  $|S(\Lambda)|_2$  пакета слота предоставляется декодеру в служебной информации. Используя длину  $|S(\Lambda)|_2$  пакета  $S(\Lambda)$  слотов и количество  $\Lambda$  слотов, декодер определяет длину  $v$  слота:

$$v = \frac{|S(\Lambda)|_2}{\Lambda}.$$

Информация о длине слота позволяет определить позиционирование всех слотов  $s_\lambda$  в пакете  $S(\Lambda)$ . Порядок заполнения слотов  $s_\xi$  предоставляет возможность идентифицировать начало  $\alpha_\xi$  каждого кода  $\ell_\xi$ , как указано на рис. 12.

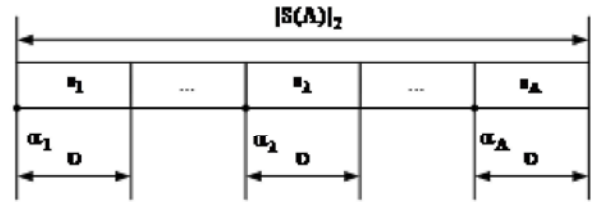


Рис. 12. Процесс разделения пакета  $S(\Lambda)$  слотов  $s_\lambda$  и определения начала  $\alpha_\lambda$  кодов  $\ell_\lambda$

Это позволяет декодеру синхронизироваться с потоком битов в начале каждого слота.

Из пакета  $S(\Lambda)$  выделяется отдельный слот  $s_\xi$  и производится процесс поразрядной сборки VLC-кода  $\ell_\xi$ . При поразрядной сборке первого VLC-кода  $\ell_1$  индекс позиции VLC-кода  $\ell_\xi$  в кодовом потоке принимается равным  $\xi = 1$ .

На первоначальном этапе  $g = 1$  старшему разряду  $q_{\xi,1}$  кода  $\ell_\xi$  приводится в соответствие значение двоичного разряда  $h_{\xi,1}$  нижней битовой позиции слота  $s_\xi$ , т.е.:

$$q_{\xi,1} := h_{\xi,1}. \quad (10)$$

При этом данный разряд формирует содержимое части кода  $\partial \ell_\xi$ :

$$[\partial \ell_\xi]_2 = \{q_{\xi,1}\}.$$

В результате этого длина  $|\partial \ell_\xi|_2$  части кода  $\partial \ell_\xi$  равняется:

$$|\partial \ell_\xi|_2 = 1.$$

После этого декодер на основе функции  $f_{\text{vlc}}^{-1}(\partial l_{\xi}, P_{\text{сл}})$  производит идентификацию окончания  $\xi$ -й кодовой комбинации  $l_{\xi}$ .

Успешная идентификация приводит к таким последствиям:

- а) кодовой комбинации  $l_{\xi}$  приводится в соответствие часть кода  $\partial l_{\xi}$ :  $l_{\xi} := \partial l_{\xi}$ ;
- б) восстанавливается соответствующая компонента  $u_{\xi}$ ;
- в) фиксируется длина  $|\partial l_{\xi}|_2$  части кода  $\partial l_{\xi}$ ;
- г) дальнейшая сборка VLC-кода  $l_{\xi}$  прекращается.

Если идентификация окончания  $\xi$ -й кодовой комбинации  $l_{\xi}$  не удалась, то разряду  $q_{\xi,2}$  кода  $l_{\xi}$  приводится в соответствие двоичный разряд  $h_{\xi,2}$  следующей битовой позиции слота  $s_{\xi}$ , т.е.:

$$q_{\xi,2} := h_{\xi,2}. \quad (11)$$

При этом изменяется содержимое  $[\partial l_{\xi}]_2$  части кода  $\partial l_{\xi}$ :  $[\partial l_{\xi}]_2 = \{q_{\xi,1}; q_{\xi,2}\}$ .

Соответственно длина  $|\partial l_{\xi}|_2$  части кода  $\partial l_{\xi}$  при этом увеличивается:  $|\partial l_{\xi}|_2 := |\partial l_{\xi}|_2 + 1$ .

После этого декодер на основе функции  $f_{\text{vlc}}^{-1}(\partial l_{\xi}, P_{\text{сл}})$  повторно производит идентификацию окончания  $\xi$ -й кодовой комбинации  $l_{\xi}$ .

Данные операции первоначального этапа побитного внесения двоичных разрядов  $h_{\xi,\mu}$  слота  $s_{\xi}$  в содержимое части кода  $\partial l_{\xi}$  продолжают до момента:

- 1) идентификации окончания  $\xi$ -й кодовой комбинации  $l_{\xi}$ ;
- 2) использования всех двоичных разрядов  $h_{\xi,\mu}$  слота  $s_{\xi}$ .

В первом случае декодер восстанавливает соответствующую компоненту  $u_{\xi}$ . Также при этом формируется избыточная составляющая  $\Delta s_{\xi}$  слота  $s_{\xi}$ . Она задается следующим образом:

$$[\Delta s_{\xi}]_2 = \{h_{\xi,|\ell_{\xi}|_2+1}; \dots; h_{\xi,\nu}\}. \quad (12)$$

В данной формуле  $h_{\xi,\mu}$  –  $\mu$ -й разряд слота  $s_{\xi}$ .

Длина  $|\Delta s_{\xi}|_2$  избыточной составляющей слота  $\Delta s_{\xi}$  находится как разница длины  $\nu$  слота  $s_{\xi}$  и длины  $|\ell_{\xi}|_2$  идентифицированного кода  $l_{\xi}$ :

$$|\Delta s_{\xi}|_2 = \nu - |\ell_{\xi}|_2.$$

Во втором случае процесс дальнейшей поразрядной сборки VLC-кодов  $l_{\xi}$  требует обращения к содержимому избыточных составляющих  $\Delta s_i$  других слотов  $s_i$ ,  $i \neq \xi$ . Это обращение производится только после идентификации других VLC-кодов  $l_i$ ,  $i \neq \xi$ , т.е. выполнения этапа  $g = 1$  на позициях всех слотов  $s_i$ .

Значения позиций данных избыточных составляющих  $\Delta s_i$  слотов  $s_i$  в последовательности  $S(\Lambda)$  задается индексом VLC-кода  $l_{\xi}$  и вектором смещения  $D(\nu_{\text{см}})$ .

При этом внесения двоичных разрядов  $h_{\xi+d_g,\mu}$  избыточных составляющих  $\Delta s_{\xi+d_g}^{(\gamma)}$  слота  $s_{\xi+d_g}$  в содержимое части кода  $\partial l_{\xi}$  продолжают до идентификации окончания  $\xi$ -й кодовой комбинации  $l_{\xi}$ . Следует заметить, что каждый этап сборки VLC-кодов  $l_{\xi}$  должен происходить после завершения предыдущего на позициях всех слотов  $s_i$ .

Результат формирования кода  $l_{\xi}$  при обращении к битовым составляющим нескольких слотов представлен на рис. 13.

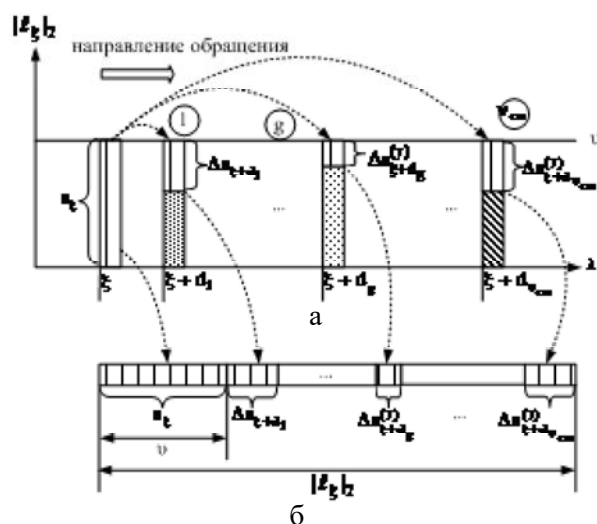


Рис. 13. Сборка VLC-кода  $l_{\xi}$  по подпоследовательности  $\Delta S(\nu_{\text{см}})$  до идентификации окончания кодовой комбинации  $l_{\xi}$ : а – изъятие битовых составляющих других слотов  $s_{\xi+d_g}$ ; б – результат формирования кода  $l_{\xi}$



Выражение (10) позволяет производить параллельную обработку всех слотов  $s_\xi$  в пакете  $S(\Lambda)$ . Остаточная избыточность битов, которые использовались при формировании пакета  $S(\Lambda)$  слотов  $s_\xi$ , на результат декодирования не влияют. Результатом обработки всех слотов  $s_\xi$  в пакете  $S(\Lambda)$  является восстановление всех компонент  $u_\xi$  линейризованной трансформанты.

При наличии битовой ошибки в  $\mu$ -м разряде  $h'_{\lambda,\mu}$   $\lambda$ -го слота  $s_\lambda$ :  $h'_{\lambda,\mu} \neq h_{\lambda,\mu}$

процесс декодирования будет зависеть от битового положения в слоте:

1) Если идентификация  $\lambda$ -й кодовой комбинации  $\ell_\lambda$  до считывания разряда  $h_{\lambda,\mu}$  слота  $s_\lambda$  не была произведена, то возможна неверная идентификация окончания  $\lambda$ -й кодовой комбинации  $\ell'_\lambda$ .

2) При идентификации  $\lambda$ -й кодовой комбинации  $\ell_\lambda$  ошибка затрагивает избыточную составляющую  $\Delta s_\lambda^{(\gamma)}$  слота  $s_\lambda$ , к которой идет обращение при сборке на  $g$ -м этапе  $\xi$ -го кода  $\ell_\xi$ ,  $\xi = \lambda - d_g$ . При этом также возможна неверная идентификация окончания  $\xi$ -й кодовой комбинации  $\ell'_\xi$ . Идентификация кода  $\ell_\lambda$  и  $\ell_i$  кодов  $\ell_i$ , избыточные составляющие которых входят в избыточные составляющие  $\Delta s_\lambda^{(j)}$ ,  $j < \gamma$  слота  $s_\lambda$ , будет произведена верно.

Для первого варианта положения ошибочного разряда  $h'_{\lambda,\mu}$  при изменении длины  $|\ell'_\lambda|_2$  кодовой комбинации  $\ell'_\lambda$ :

а) в сторону увеличения  $|\ell'_\lambda|_2 > |\ell_\lambda|_2$  ошибка распространяется на коды  $\ell_i$ , которые при сборке должны были использовать разряды слотов  $s_i$  с позицией  $i \in \{\lambda + d_{v_{cm}}; \dots; \lambda + d_{v'_{cm}}\}$  и битовое положение в слоте после избыточной составляющей  $\ell'^{(v'_{cm})}_\lambda$  кода  $\ell'_\lambda$ ;

б) в сторону уменьшения  $|\ell'_\lambda|_2 < |\ell_\lambda|_2$  ошибка распространяется на коды  $\ell_i$ , которые при сборке будут использовать разряды слотов  $s_i$  с позицией  $i \in \{\lambda + d_{v'_{cm}}; \dots; \lambda + d_{v_{cm}}\}$  и битовое положение в слоте после избыточной составляющей  $\ell^{(v_{cm})}_\lambda$  кода  $\ell'_\lambda$ .

При втором варианте положения ошибочного разряда  $h'_{\lambda,\mu}$  ситуация повторяется для кода  $\ell'_\xi$ .

Наглядное представление неверного декодирования пакета слотов с рис. 11 при ошибке разряда 5 в слоте 1 показано на рис. 14.

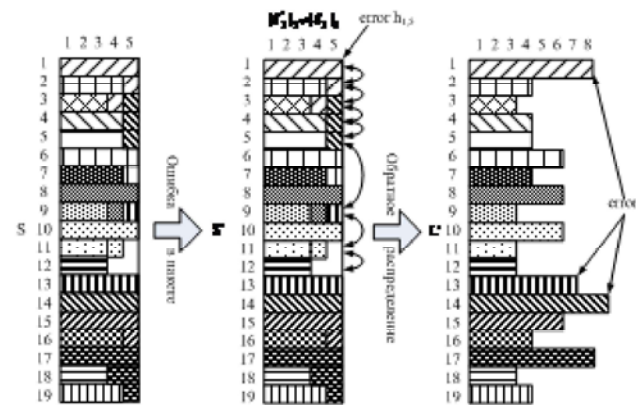


Рис. 14. Влияние ошибки в разряде  $h_{1,5}$  слота  $s_1$  на определение длин  $|\ell_i|_2$  кодов  $\ell_i$  последовательности  $L(\theta)$

В случае ошибочного декодирования первого кода  $\ell_1$  декодер неверно определит длину первого кода. Для обратного распределения коды с 2 по 12 и с 15 по 19 останутся незатронутыми. Для кодов 1, 13 и 14 декодер может использовать как предыдущие, так и следующие значения разрядов, определенных алгоритмом распределения.

В результате ошибка в слоте 1 приведет к неверному декодированию блоков 1, 13 и 14. При отсутствии распределения блоков по слотам ошибка распространилась бы на все кодируемые блоки. В результате достигается локализация потери целостности информации на основе слот-технологии.

Обратно-пропорциональная зависимость длины статистического кода от частоты его появления позволяет при использовании слот-технологии защитить от битовой ошибки ВЧ компоненты трансформанты [8]. При этом лавинный эффект ошибки для НЧ компонент изображения устранить полностью не удастся. Для его устранения предлагается использовать изменяющуюся избыточность распределения с механизмом обратной связи между кодером и декодером.

#### 4. Выводы

- 1) Разработан метод локализации потери целостности информации на основе слот-технологии при незначительном увеличении длины пакета, который необходим для кодирования компонент.
- 2) Создана технология, которая учитывает применение кибератак на видеoinформационный ресурс.
- 3) Для локализации ошибки декодирования для НЧ компонент впервые предложено использовать дина-

мическую избыточность технологии распределения с механизмом обратной связи между кодером и декодером.

**Литература: 1.** Баранник В.В., Подлесный С.А. / Анализ действия кибератак на видеоинформационный ресурс в информационно-телекоммуникационных сетях // АСУ и приборы автоматики. Вып. 164. 2014. С. 16-22 **2.** Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007. № 537-V **3.** [Електронний ресурс] [http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art\\_id=104662&cat\\_id=38712](http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712), 2012. **4.** Звіт CERT-UA за 2014 рік, [Електронний ресурс], <http://cert.gov.ua/?p=2019>, 2015. **5.** 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>, Киев, 2012. 190 с. **6.** Richardson E. H.264 and MPEG-4 video compression. Chichester, UK: Wiley and Sons, 2003. 306 p. **7.** Wang Y. and Zhu Q. F. Error control and concealment for video communication: A review // Proceedings of the IEEE. Vol. 86. no. 5. P. 974-997. May 1998 **8.** Баранник В.В., Подлесный С.А. / Обґрунтування підходу щодо створення технології кіберзахисту відеоінформаційного ресурсу в інфокомунікаційному просторі дії кібератаки на відеоінформаційний ресурс в інформаційно-телекомунікаційних мережах // Радіоелектроніка та інформатика. 2015. №3. С.62-66.

**Transliterated bibliography: 1.** Analysis of the action of cyber-attacks in the video-information's resources in the information-telecommunications networks / V. Barannik, S. Podlesny // Management Information System and Devices. 2014. N 169. P.16-22. **2.** Zakon Ukraїni «Pro Osnovni zasady rozvitku informacijnogo suspil'stva v Ukraїni na 2007–2015 roki» vid 09.01.2007 № 537-V **3.** Zahist informacijnih mrezh є pitannjam derzhavnoї bezpeki - golova Derzhspeczv'jazku Gennadij Reznikov [Electronic resource] [http://](http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712)

[www.dstszi.gov.ua/dstszi/control/uk/publish/article?art\\_id=104662&cat\\_id=38712](http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712), 2012. 4. CERT-UA Report 2014, [Electronic resource], <http://cert.gov.ua/?p=2019>, 2015. **5.** Martynjuk I. Materialy tehničeskogo treninga «Postroenie bezopasnyh setej na oborudovanii D-Link», [Electronic resource], <http://service.d-link.ua/sites/default/files/files/Security.zip>, Kiїв, 2012. 190 p. **6.** Richardson E. H.264 and MPEG-4 video compression. Chichester, UK: Wiley and Sons, 2003. 306 p. **7.** Y. Wang and Q. F. Zhu, “Error control and concealment for video communication: A review,” Proceedings of the IEEE, vol. 86, no. 5. pp. 974-997, May 1998 **8.** Obosnovanie podhoda k sozdaniju tehnologii kiberzashhity videoinformacionnuju resursa v infokomunikacionnyh prostranstve dejstvija kiberataki na Videoinformacionnyj resurs v informacionno-telekommunikacionnyh setjah / V. Barannik, S. Podlesny // Radioelektronika i informatika. 20015. N 3. P. 62-66.

Поступила в редколлегию 08.12.2015

**Рецензент:** д-р техн. наук, проф. Безрук В.М.

**Баранник Владимир Викторович**, д-р техн. наук, профессор, начальник кафедры боевого применения и эксплуатации АСУ Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: обработка и передача информации. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79.

**Подлесный Сергей Анатоліевич**, начальник отделения ХУВС. Научные интересы: технологии кодирования и обеспечения информационной безопасности государства. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79. Email: Barannik\_V\_V@mail.ru

**Баранник Дмитрий Владимирович**, студент ХНУРЭ. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79. E-mail: barannik\_v\_v@mail.ru.