© Barannik V, Podlesny S. Method for increasing resistance of cyberattacks for video content in infocommunication system // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 123-130.

МЕТОД ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ВИДЕОКОНТЕНТА К КИБЕРНЕТИЧЕСКИМ АТАКАМ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Владимир Баранник, Сергей Подлесный

Харьковский национальный університет Воздушных Сил им. И. Кожедуба, Украина

БАРАННИК Владимир Викторович, д.т.н.

Год и и место рождения: 1971 год, г. Изюм, Харьковская область, Украина.
Образование: Харьковский военный университет, 1994 год.
Должность: начальник кафедры боевого применения и эксплуатации АСУ с 2012 года.
Научные интересы: информационная безопасность.
Публикации: более 350 научных публикаций, среди которых монографии, учебники, учебные пособия, научные статьи и патенты на изобретения.
E-mail: barannik_v_v@mail.ru

ПОДЛЕСНЫЙ Сергей Анатолиевич

Год и и место рождения: 1978 год, г. Городня, Черниговская область, Украина.
Образование: Харьковский інститут Военно-Воздушных Сил, 2001 год.
Должность: начальник кафедры боевого применения и эксплуатации АСУ с 2012 года.
Научные интересы: информационная безопасность.
Публикации: более 20 научных публикаций.
E-mail: barannik_v_v@mail.ru

Анотация. *Обосновывается важность применения видеоинформационного ресурса (ВИР). Указывается на необходимость обеспечения информационной безопасности государственного видеоинформационного ресурса. Проводится анализ влияния кибернетических угроз на потерю категорий информационной безопасности ВИР. Указывается на наличие проблемных недостатков для методов противодействия кибернетическим атакам. Аргументируется необходимость создания метода повышения устойчивости ВИР к DDoS-атакам в инфокоммуникационных системах в режимах, когда кибератаки не обнаружены или замаскированы. Указывается на наличие недостатков для существующих технологий синтаксического кодового представления видеоконтента. Показывается присутствие уязвимости позиционирования для статистического кодирования. Для устранения данной уязвимости предлагается использовать структурно-блочное кодирование. Проводится анализ состояния категорий целостности и доступности видеоконтента при наличии ошибки в кодограмме. Для повышения целостности информационного ресурса при заданной степени его доступности предлагается производить распределение кодограмм в кодовые конструкции одинаковой длины. Рассматривается влияние созданного метода на состояние информационного безопасности видеоконтента. Указывается на повышение целостности информационного ресурса при использовании созданного метода.*

Ключевые слова: *информационная безопасность, видеоинформационный ресурс, структурное кодирование, слот-технология, кибератаки.*

Вступление

В современных условиях область использования систем передачи видеоинформации охватывает различные сферы деятельности государства. Сфера применения включает системы контроля за кризисными ситуациями, системы АСУ специального назначения, ведомственные сети профильных министерств. При этом для формирования видеоинформационного ресурса (ВИР) используются системы видеоконференцсвязи и системы мониторинга. В результате достигается повышение эффективности принятия решений в системах контроля за кризисными ситуациями [4]. Важность решаемых задач придает ВИР статус государственного. Это приводит к необходимости обеспечения категорий информационной безопасности государственного видеоинформационного ресурса.

В то же время существуют угрозы потери категорий информационной безопасности вследствие проведения кибератак. Это связано с воздействием противоборствующей стороны на информационные потоки. В результате действия кибернетических атак происходит потеря целостности и доступности ви-

деоинформационного ресурса. В течение 2014 года специализированным структурным подразделением Государственного центра защиты информационно-телекоммуникационных систем (ГЦЗ ИТС) Государственной службы специальной связи и защиты информации Украины (Госспецсвязи) CERT-UA были приняты меры по реагированию на 216 компьютерных инцидентов [5]. Наиболее распространенными видами кибератак (43 для украинского государственного сектора, 2 для украинского коммерческого сектора, 3 для зарубежного государственного сектора, 3 для зарубежного коммерческого сектора) являются атаки типа DDoS-атака. Такие атаки могут осуществляться путем непосредственной пересылки большого количества пакетов (UDP, ICMP flood), использование атак на промежуточные узлы (Smurf, Fraggle), передачи слишком длинных пакетов (Ping of Death), некорректных пакетов (Land) или большого количества трудоемких запросов. Заметим, что в последнее время происходит развитие этого направления деятельности и появление новых видов и способов атак. Из последних тенденций можно отметить появление атак ухудшения качества (Quality Reduction Attack) и низкочастотных атак (Low Rated Attack) и, безусловно, этот процесс будет продолжаться, требуя новых исследований и разработки новых методов противодействия.

Основные существующие классы атак достаточно хорошо изучены. Атаки классифицированы согласно протоколам, по которым они осуществляются. Для истощения ресурсов сети выполняется пересылка большого количества пакетов в сеть жертвы. В результате происходит уменьшение ее пропускной способности для законных пользователей. Для отраженной атаки с использованием серверов доменных имен (Domain Name System (DNS) servers) с начальным трафиком запросов 140 Mb/s ботнет может привести к потоку DNS ответов мощностью 10 Gb/s. Это приводит к необходимости обработки большого потока информации телекоммуникационным устройством в существующей модели обработки и доставки видеоинформационного ресурса. Проявление результата DDoS-атаки на передачу видеоинформационного ресурса зависит от протокола передачи данных. Влияние атаки на видеопоток при UTP соединении выражается в потере пакетов, для TCP соединения: происходит задержка пакетов. Для конечного пользователя государственным ВИР наблюдается замирание видео, искажение кадра, пропадание видеоконтента. Для ведомственных учреждений данные искажения информационного ресурса являются недопустимыми. Как в случае осуществления наблюдения, так и при проведении видеоконференций это приводит к несвоевременности принятия решения в системе контроля за кризисными ситуациями. В результате наступает снижение эффективности управления в государственных ведомственных учреждениях. Поэтому существует научно-прикладная задача относительно повышения устойчивости видеоинформационного ресурса в условиях проведения DDoS-атак на видеоконтент.

Одним из направлений решения является использование технологий локализации действия кибератак и специализированного сетевого оборудования. Для предупреждения возникновения атаки типа DDoS-атака применяются системы обнаружения и предотвращения вторжений, управляемые коммутаторы со списками контроля доступа и резервирования линий связи между отдельными узлами [8]. Перечисленные методы обладают такими недостатками, как: вносимые через обработку пакетов задержки и, как результат, ограничение скорости передачи сигнала в сети; увеличенная стоимость оборудования и подписки на сигнатуры; невозможность обеспечения защиты от замаскированных вирусных атак.

При этом не обеспечивается противодействие атаке на ее начальном этапе или при случае невозможности ее идентификации. Это приводит к проблеме наличия задержек передачи пакетов, что выражается в потере целостности и доступности ВИР. Здесь требуется отметить, что даже в условиях отсутствия кибератак при функционировании телекоммуникационных устройств происходят потери видеоинформационного ресурса. К примеру, вероятность потери бита информации при передаче в нормальных условиях в проводных системах составляет около 10^{-8}, а для беспроводных систем составляет около 10^{-3} [7]. Поэтому **цель работы** заключается в создании метода повышения устойчивости видеоинформационного ресурса к DDoS-атакам в инфокоммуникационных системах в режимах, когда кибератаки не обнаружены или замаскированы.

Разработка метода повышения устойчивости видеоинформационного ресурса

Одним из направлений достижения поставленной цели является разработка метода синтаксического представления видеоинформационного ресурса для обеспечения категорий целостности и доступности ВИР в условиях действия кибератак. Существующие методы представления видеоинформационного ресурса основываются на использовании статистического кодирования [6]. Данному кодированию присущи следующие недостатки:

1. В случае наличия ошибки в кодовом представлении компоненты трансформанты, при котором сохраняется позиционирование кодовых слов в потоке, восстановленной компонента присвоится ошибочное значение. Это приводит к потере доступности ВИР.

2. Для ошибки в кодовом представлении компоненты трансформанты, при которой происходит смещение кодовых слов в потоке, характерно отсутствие возможности восстановления последующих компонент. В результате происходит потеря доступности ВИР. Уязвимости категорий информационной безопасности связаны с особенностями позиционирования статистического кода. Для существующих технологий кодирования не предоставляется возможным предварительно производить разделение кодового потока на кодовые слова. Для устранения данного недостатка предлагается применять структурно-блочное кодирование. При этом происходит

снижение количества разрядов на кодовое представление массивов видеоданных [1]. Важным свойством структурно-кодированных чисел является возможность вычисления кода для массива данных на основе аналитического выражения. Для этого необходимо знать только значения элементов массива данных и значения компонент вектора оснований. В результате отсутствует необходимость организовывать формирование таблицы допустимых чисел и проводить поиск в таблице необходимого индекса, соответствующего обрабатываемому числу [2].

При использовании структурно-блочного кодирования происходит уменьшение количества структурной избыточности [3].

Рассмотрим подробнее процесс обработки изображения при помощи структурного кодирования. Первоначально кадр изображения представляет собой массив пикселей размерностью $M \times N$. Количество δ градаций яркости элементов цветовой компоненты изображения характеризует максимально возможное значение яркости X. Исходный кадр изображения перед обработкой разбивается на сегменты X_φ (рис. 1).

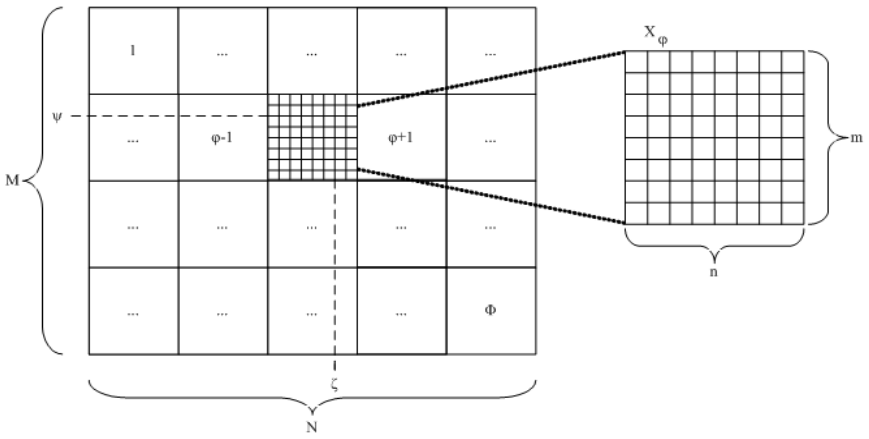

Рис. 1. Представление сегментированного изображения

Индекс φ сегмента X_φ в кадре определяется с помощью координатных переменных ψ и ζ, что задается таким выражением:

$$\varphi = (\psi - 1) \times \zeta_{max} + \zeta, \qquad \varphi = \overline{1, \Phi},$$

где ψ – координата сегмента X_φ в кадре по вертикали и ζ – координата сегмента X_φ в кадре по горизонтали; $\psi_{max} = \frac{M}{m}$ – максимальное значение координатной переменной по вертикали; Φ – количество сегментов X_φ в кадре.

Максимальное значение координатной переменной по вертикали ψ_{max} и по горизонтали $\zeta_{max} = \frac{N}{n}$ определяется из соотношения размера кадра и сегмента.

Над значениями яркости сегментов X_φ производится дискретно-косинусное преобразование с формированием массива трансформанты Y_φ:

$$X_\varphi \xrightarrow{DCT} Y_\varphi .$$

Процесс формирования кодовой последовательности описывается следующим порядком. Кодированию подлежат значения компонент трансформанты Y. Они характеризуются динамическим диапазоном строк Δ_k компонент $y_{k\ell}$:

$$\Delta_k = y_{k,max} + 1, \qquad (1)$$

где Δ_k – величина диапазона компоненты $y_{k\ell}$; $\Delta_{k,max}$ – величина диапазона k-ой строки трансформанты Y.

При одномерном кодировании для каждого столбца трансформанты формируется значение кодограммы согласно следующей формулы:

$$K_\ell = \sum_{i=1}^{\alpha} y_{i\ell} \times \rho_i , \qquad (2)$$

где $y_{i\ell}$ – значение компоненты трансформанты для ℓ-го столбца; ρ_i – величина накопленного произведения для i оснований.

Значение накопленного произведения определяется из значений $\Delta_{k,max}$ величины диапазона k-ой строки трансформанты Y согласно выражению:

$$\rho_i = \prod_{k=i+1}^{\alpha} \Delta_{k,max} . \qquad (3)$$

Наглядно процесс формирования кодограммы показан на рис. 2.

Система оснований позволяет определить верхнюю границу ρ_{max} значения кода одномерного числа кодограммы согласно неравенства:

$$K_{max}^{(\varphi)} < \rho_{max},$$

где $K_{max}^{(\varphi)}$ – максимально возможное значение кода для заданного вектора оснований $E^{(\varphi)}$.

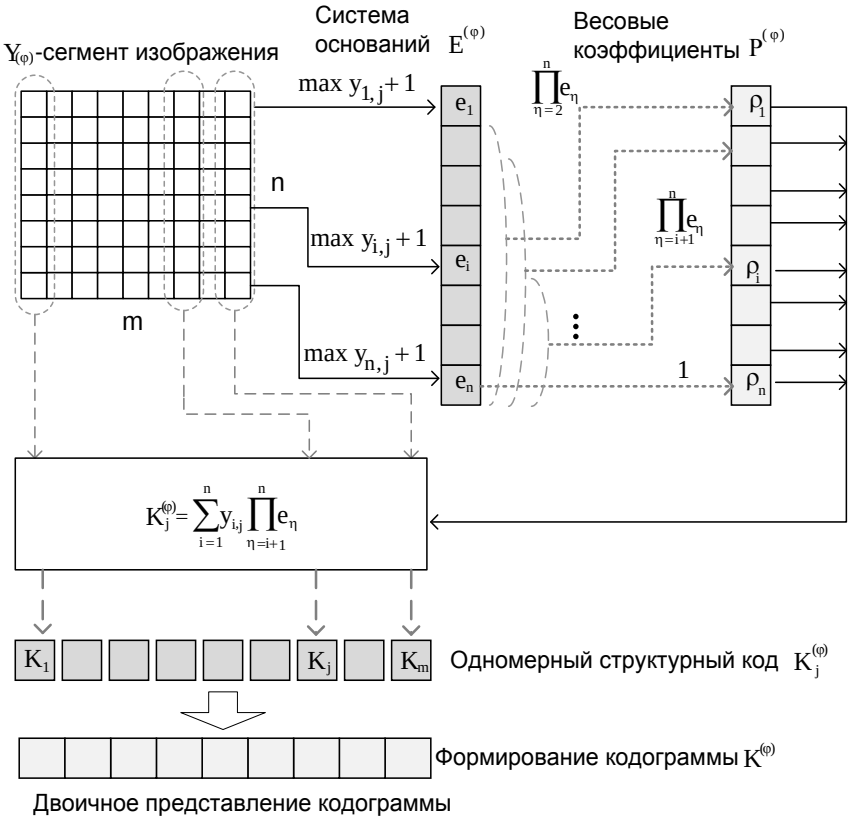

Рис. 2. Схематическое представление структурного кодирования

Знание верхней границы ρ_{max} необходимо для определения длины кодового представления $d_i^{(\varphi)}$ одной компоненты $Y_i^{(\varphi)}$ трансформанты. В этом случае принимается условие:

$$d_i^{(\varphi)} = [\log_2 \rho_{max}] + 1, \quad (4)$$

где $d_i^{(\varphi)}$ – длина кодового представления i-го столбца трансформанты; $[\log_2 \rho_{max}]+1$ – количество двоичных разрядов на представление максимального значения кода $K_{max}^{(\varphi)}$ одномерного числа кодограммы.

Тогда длина $d_{inf}^{(\varphi)}$ всей информационной части кодовой последовательности составит:

$$d_{inf}^{(\varphi)} = m \times ([\log_2 \rho_{max}] + 1),$$

где m – количество столбцов трансформанты; $m \times ([\log_2 \rho_{max}]+1)$ – количество разрядов на представление m кодов кодограммы.

Зная длину кодового представления для одного столбца массива промежуточных результатов обработки изображения в неравномерном базисе спектральных коэффициентов, получаем возможность определить длину $d_{inf}^{(\varphi)}$ информационной части кодовой последовательности массива промежуточных результатов обработки изображения. Она соответствует сумме длин кодовых представлений всех столбцов массива промежуточных результатов обработки изображения, т.е.

$$d_{inf}^{(\varphi)} = m \times d_i^{(\varphi)} = m([\log_2 \prod_{\eta=1}^{n} e_\eta] + 1). \quad (5)$$

Кодовая последовательность формируется на приемной стороне на основе полученных пакетов данных (рис. 3). Структура пакета подразумевает наличие служебной (СЧ) и информационной частей (ИЧ), а кодограммы формируются на основе информационных частей пакетов данных.

Длина $d^{(\varphi)}$ собранной кодовой последовательности всего массива промежуточных результатов обработки изображения определяется как количество бит, которым представлена служебная часть $d_s^{(\varphi)}$ и длина $d_{inf}^{(\varphi)}$ кодового представления всех столбцов трансформанты, она выражается формулой:

$$d^{(\varphi)} = d_s^{(\varphi)} + d_{inf}^{(\varphi)}. \quad (6)$$

Для проведения декодирования чисел необходимо выделить служебную и информационную части собранной кодовой последовательности. Это вызвано тем, что длина информационной части может изменяться для разных сегментов трансформированного изображения. Длина информационной части кодового представления трансформанты может изменяться из-за того, что: размеры сегментов изображения могут быть различными; сегменты изображения могут иметь разную систему оснований, что объясняется разной содержательной частью трансформанты изображения (рис. 4).

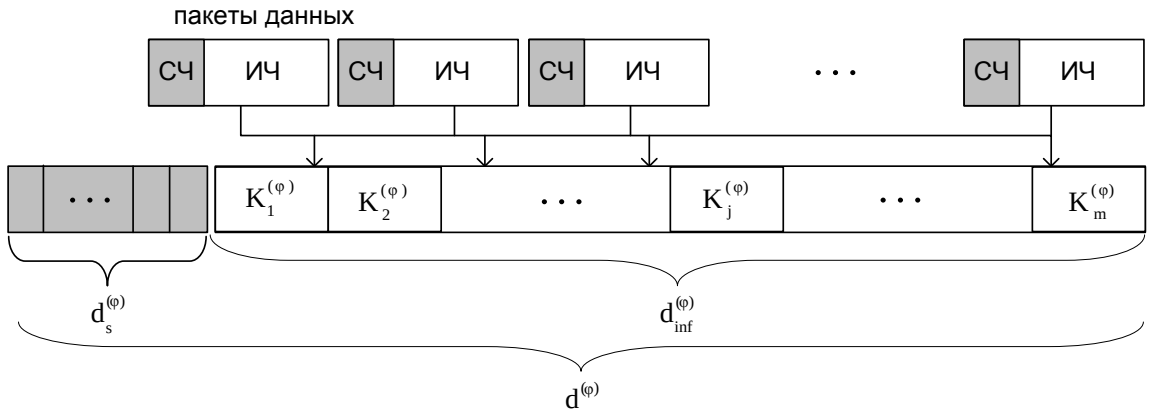

Рис. 3. Технология определения информационной и служебной части массива промежуточных результатов обработки изображения

Выборка информационной части из общей кодовой последовательности производится исходя из особенностей построения кода. Технология определения информационной части заключается в том, чтобы в общей длине кодовой последовательности определить границу служебной части.

Для этого не обходимо принять значение величины служебной части $d_{s,j}^{(\varphi)}$ кодового представления числа кодограммы для одной j-го столбца (φ) массива промежуточных результатов обработки изображения b (например, $b=8$).

Длина кодового представления элемента основания составит:

$$d_{s,1}^{(\varphi)} \ldots = \ldots d_{s,j}^{(\varphi)} \ldots = \ldots d_{s,n}^{(\varphi)} = \log_2 b . \quad (7)$$

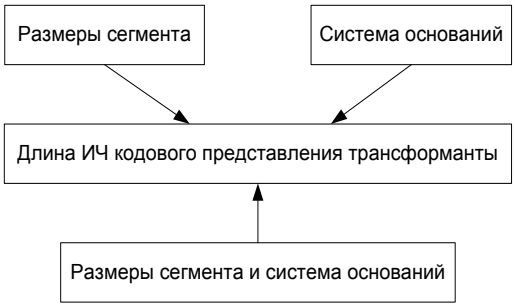

Рис. 4. Основные условия, влияющие на длину информационной части кодового представления массива промежуточных результатов обработки сегмента изображения

Тогда длина служебной части $d_s^{(\varphi)}$ всей кодовой последовательности трансформанты ДКП соответственно определяется длинами кодовых представлений всех элементов основания:

$$d_s^{(\varphi)} = n \times d_{s,j}^{(\varphi)} = n \times \log_2 b , \quad (8)$$

где n – количество строк массива промежуточных результатов обработки изображения.

Выделить из собранной кодовой последовательности служебную часть. Первый бит всей кодовой последовательности является служебным, а длина ее служебной части составляет $n \log_2 b$ бит. Следующий за ним $n \log_2 b + 1$ бит будет информационным.

Позиция первого бита кодового представления следующей трансформанты относительно текущей определяется как

$$P_1^{(\varphi+1)} = P^{(\varphi)} + 1 , \quad (9)$$

где $P^{(\varphi)}$ – последняя позиция кодограммы предыдущей трансформанты, которая находится как:

$$P^{(\varphi)} = n \log_2 b + m([\log_2 \prod_{\eta=1}^{n} e_\eta] + 1) . \quad (10)$$

Таким образом, нет необходимости использования маркеров-разделителей для разделения служебной и информационной частей кодовой конструкции при условии отсутствия ошибок в канале.

Восстановление компонент трансформанты из кодограммы происходит по следующей формуле:

$$y_{i\ell} = \lfloor \mathrm{mod}(K_\ell / \rho_{i-1}) / \rho_i \rfloor , \quad (11)$$

где $\mathrm{mod}(K_\ell / \rho_{i-1})$ – остаток от деления значения кодограммы K_ℓ на значение накопленного произведения ρ_{i-1} для предыдущей строки; $\lfloor a/b \rfloor$ – определение целого частного от деления.

Рассмотрим влияние битовой ошибки в кодограмме на процесс декодирования.

Исходя из порядка формирования кодограммы (2) при наличии ошибки в информационной части количество искаженных компонент трансформанты определяется позицией ошибки. Наглядно количество восстановленных с искажением компонент столбца трансформанты для разных областей позиций ошибки представлено на рис. 5.

Искаженные компоненты столбца трансформанты на рис. 5. графически обозначены серой областью. При этом происходит потеря целостности ВИР. Из этого следует, что при искажении младших бит кодограммы ошибка повлияет на компоненты трансформанты, которые соответствуют нижней позиции столбца. Для ошибки в старших битах кодограммы характерно искажение всего столбца. При этом на компоненты других столбцов ошибка не влияет.

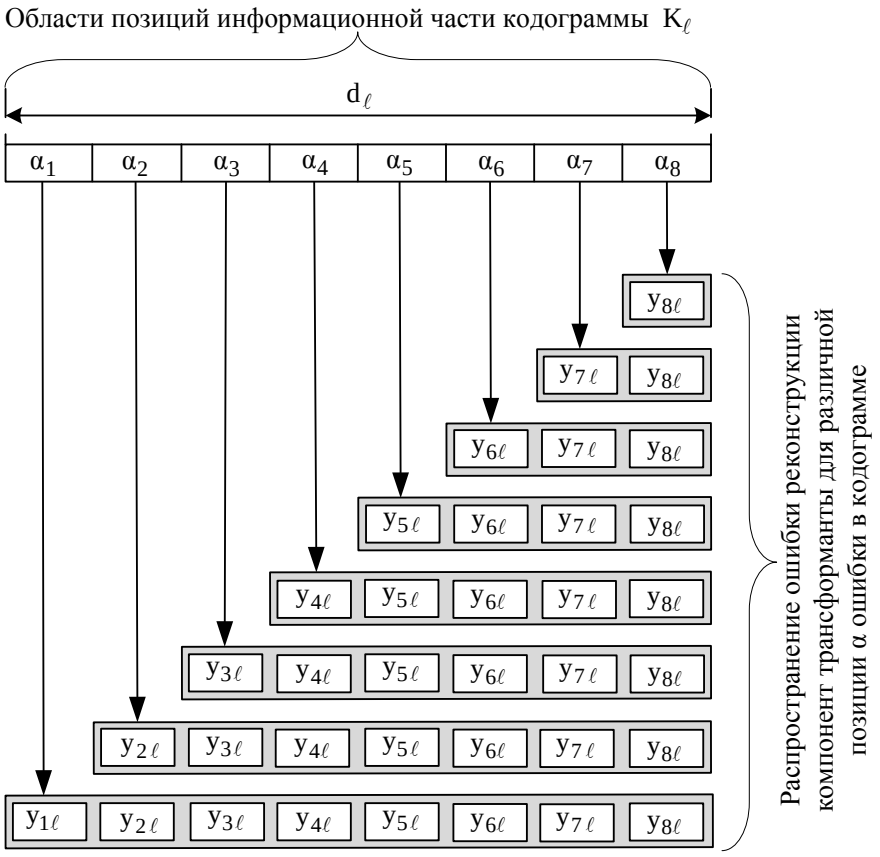

Рис. 5. Влияние позиции искаженного бита информационной части кодограммы на количество восстановленных с ошибкой компонент трансформанты

При наличии ошибки в служебной части приводит к искажению значения восстановленных компонент трансформанты и неверному позиционированию смещению определяется позицией ошибки первого бита кодового представления следующей трансформанты относительно текущей. В результате наступает потеря целостности ВИР.

Для устранения нарушения целостности видеоинформационного ресурса предлагается производить перераспределение содержимого кодограмм трансформант в кодовые конструкции одинаковой длины.

В связи с тем, что служебная часть трансформанты согласно (8) имеет фиксированную длину, распределению необходимо подвергать информационную часть кодограмм.

Суммарное количество сегментов, кодовые представления трансформант которых помещаются в один слот, имеет значение υ. На рис. 6 схематически представлено распределение кодограмм трансформант для номера сегмента от $(\varphi+1)$ до $(\varphi+\upsilon)$ для трансформационного представления одного кадра.

Для обеспечения позиционирования необходимо рассчитать длину одного слота. Она определяется по формуле:

$$|S^{(\phi)}|_2 = \frac{1}{\upsilon}\cdot\sum_{j=\phi+1}^{\phi+\upsilon} d_{\inf}^{(j)} = \left\lceil \frac{m}{\upsilon}\cdot\sum_{j=\phi+1}^{\phi+\upsilon}(\log_2\prod_{i=1}^{n} e_i^{(j)}+1)\right\rceil.$$

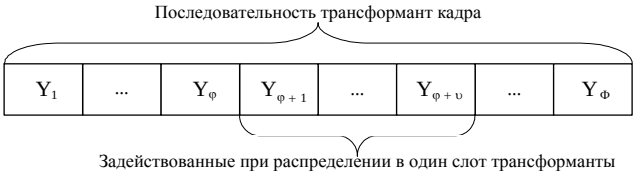

Рис. 6. Представление сегментированного изображения

Из этого следует, что при кратности количества m столбцов в трансформанте количеству υ распределяемых трансформант избыточность распределения равняется нулю, т.е.:

$$\delta = \upsilon\times|S^{(\phi)}|_2 - \sum_{j=\phi+1}^{\phi+\upsilon} d_{\inf}^{j} = 0.$$

Данная технология задается функцией преобразования f_{erec}. Это определяется следующим выражением:

$$K^{(j)} \xrightarrow{f_{erec}} S^{(j)}, \quad j=(\varphi+1,\ \ldots,\ \varphi+\upsilon)\ . \quad (12)$$

Здесь f_{erec} – функция распределения кодограмм $K^{(j)}$ в слоты $S^{(j)}$, υ – количество слотов, в которые распределены кодограммы.

Порядок заполнения слотов показан на рис. 7.

Информацию о сумме длин информационных частей кодограмм $\sum_{j=\varphi+1}^{\varphi+\upsilon} d_{inf}^{(j)}$ для сегмента от $(\varphi+1)$ до $(\varphi+\upsilon)$ необходимо передавать по защищенному каналу. Составляющие информационных частей кодограмм, которые не вошли в слот в силу превышения длины информационной части кодограммы над длиной слота $d_{inf}^{(j)} > |S^{(\varphi)}|_2$ необходимо внести в слоты с отрицательной избыточностью. Однозначность позиционирования старших разрядов кодограмм трансформант обеспечивается за счет защищенности значения суммы длин информационных частей кодограмм $\sum_{j=\varphi+1}^{\varphi+\upsilon} d_{inf}^{(j)}$ для пакета сегментов от $(\varphi+1)$ до $(\varphi+\upsilon)$ и фиксированного количества υ сегментов в пакете.

В связи с возможностью позиционирования кодограмм при помощи предложенного метода рассмотрим влияние ошибок в служебной части кодограмм на обеспечение состояния информационной безопасности. Однозначность позиционирования старших разрядов информационной части кодограмм устраняет потерю доступности содержимого компонент трансформант.

Ошибка в служебной части кодограммы $(\varphi+j)$ сегмента влияет только на восстановление $Y^{(\varphi+j)}$ трансформанты. Также она затрагивает младшие разряды информационных частей кодограмм $K^{(\varphi+i)}$, $i \neq j$, которые были распределены в слот S_j.

Изменения данных младших разрядов приводят к неверному декодированию компонент, которые располагаются в правом нижнем углу трансформанты $Y^{(\varphi+i)}$, $i \neq j$. В целом это приводит к локализации распространения ошибки в пределах пакета сегментов от $(\varphi+1)$ до $(\varphi+\upsilon)$. С помощью этого достигается повышение доступности видеоинформационного ресурса. Полученные преимущества примененной методики при этом достигаются затратами на передачу по защищенному каналу информации о сумме длин информационных частей кодограмм $\sum_{j=\varphi+1}^{\varphi+\upsilon} d_{inf}^{(j)}$ для пакета сегментов от $(\varphi+1)$ до $(\varphi+\upsilon)$.

В связи с отсутствием необходимости производить вычисление длины информационной части $d_{inf}^{(\varphi)}$ кодограмм трансформанты предоставляется возможность производить параллельное декодирование компонент для различных трансформант для пакета сегментов от $(\varphi+1)$ до $(\varphi+\upsilon)$. Результатом такого распределения является снижение таких параметров оценки качества воспроизведения видео как задержка $T_{ЗП}$ и джиттер пакетов ∂. Уменьшение количества $\nu_{ПП}$ потерянных пакетов при локализации распространения ошибки приводит к повышению состояния информационной безопасности видеоконтента.

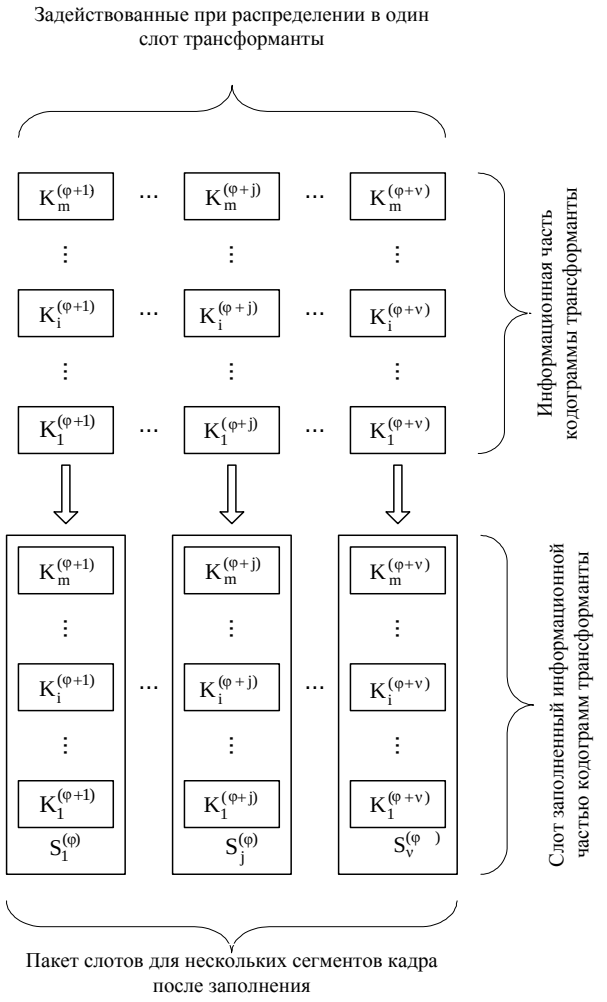

Рис. 7. Порядок заполнения содержимым информационных частей кодограмм в слоты

Выводы

1. Обоснована необходимость обеспечения целостности информационных потоков в условиях действия кибератак на государственный ВИР.

2. Проведен анализ угроз информационной безопасности при осуществлении кибератак на ВИР.

3. Обоснована необходимость повышения устойчивости видеоинформационного ресурса в условиях проведения DDoS-атак.

4. Создан метод повышения устойчивости информационного ресурса путем распределения информационной части структурно-блочного представления видеоконтента в слоты одинаковой длины.

5. Произведена оценка действия битовых ошибок на процесс восстановления ВИР из кодовых конструкций, сформированных при структурно-блочном кодировании.

6. Использование созданного метод синтаксического представления информационного ресурса

приводит к повышению категории целостности при заданной степени его доступности.

Литература

[1] Баранник В.В., Гулак Н.К., Королева Н.А. Метод сжатия изображений на основе неравновесного позиционного кодирования битовых плоскостей [Текст], Радіоелектронні і комп'ютерні системи. Х.: ХНАУ «ХАІ», 2009. – Вип. 1. – С. 55-61.

[2] Баранник В.В. Кодирование трансформированных изображений в инфокоммуникационных системах [Текст] / В.В. Баранник, В.П. Поляков. Х.: ХУПС, 2010. – С. 212.

[3] Баранник В.В., Кулица О.С., Туренко С.В. Метод повышения доступности видеоинформации аэромониторинга, Радиоэлектронные и компьютерные системы. – 2013. – № 3 (62). – С. 53-58.

[4] Баранник В.В., Подлесный С.А. Анализ действия кибератак на видеоинформационный ресурс в информационно-телекоммуникационных сетях, АСУ и приборы автоматики: научно-технический сборник. – Вып. 169. – Х.: ХНУРЭ. – 2014. – С. 16-22.

[5] Звіт CERT-UA за 2014 рік [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?p=2019.

[6] Красильников Н.Н. Цифровая обработка изображений. [Текст] / М.: Вузовская книга, 2011. – 320 с.

[7] Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. [Текст] / В.Г. Олифер, Н.А. Олифер. СПб.: Питер, 2006. – 958 с.

[8] Мартынюк И. Материалы технического тренинга «Построение безопасных сетей на оборудовании D-Link» [Електронный ресурс]. – Режим доступа: http://service.d-link.ua/sites/default/files/files/Security.zip.

УДК 621.39 (045)

Баранник В.В., Підлісний С.А. Метод підвищення стійкості відеоконтенту до кібернетичних атак у інфокомунікаційних системах

Анотація. *Обґрунтовується важливість застосування відеоінформаційного ресурсу (ВІР). Вказується на необхідність забезпечення інформаційної безпеки державного відеоінформаційного ресурсу. Проводиться аналіз впливу кібернетичних загроз на втрату категорій інформаційної безпеки ВІР. Вказується на наявність проблемних недоліків для методів протидії кібернетичним атакам. Аргументується необхідність створення методу підвищення стійкості ВІР до DDoS-атакам в інфокомунікаційних системах в режимах, коли кібератаки не виявлені або замасковані. Вказується на наявність недоліків для існуючих технологій синтаксичного кодового подання відеоконтенту. Показується присутність уразливості позиціонування для статистичного кодування. Для усунення даної уразливості пропонується використовувати структурно-блочне кодування. Проводиться аналіз стану категорій цілісності і доступності відеоконтенту за наявності помилки в кодограмі. Для підвищення цілісності інформаційного ресурсу при заданому ступені його доступності пропонується проводити розподіл кодограм в кодові конструкції однакової довжини. Розглядається вплив створеного методу на стан інформаційного безпеки відеоконтенту. Вказується на підвищення цілісності інформаційного ресурсу при використанні створеного методу.*

Ключові слова: *інформаційна безпека, відеоінформаційний ресурс, структурне кодування, слот-технологія, кібератака.*

Barannik V., Podlesny S. Method for increasing resistance of cyberattacks for video content in infocommunication system

Abstract. *The importance of applying an video information resource (VIR) is substantiated. Indicates the need for ensuring the information security of the state video information resource. The impact of cyber threats to loss categories of information security of VIR is analyzed. It indicates the presence of problematic deficiencies for countering cyber attacks methods. The necessity of creating a method of increasing resistance VIR to DDoS-attacks in the info-communication systems in modes where cyber attacks are not detected or masked is proved. It indicates the presence of deficiencies of existing technologies for syntactic code representation of video content. It shows the presence the vulnerability of position for entropy coding. The structural-block coding is proposed to use to fix this vulnerability. The status categories of integrity and availability of video content in the presence of errors in the code is analyzed. To enhance the integrity of the information resource for a given degree of availability proposed to produce distribution of code in the structure of equal length. Examines the impact of the created method to the condition of information security video. It indicates an increase of the integrity of the information resource by using the created method.*

Key words: *information security, video information resource, structural coding, slot technology, cyber attacks.*

Отримано *13 травня 2016 року*, затверджено редколегією *27 травня 2016 року*