УДК: 621.396 DOI: 10.53816/23061456\_2022\_7–8\_22

# АЛГОРИТМ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ДОСТАВКИ ДАННЫХ ПО СПУТНИКОВОМУ СТЕГОКАНАЛУ С УЧЕТОМ ПОТЕРЬ

**В СРЕДЕ ПЕРЕДАЧИ**

# ALGORITHM OF THE ENSURING RELIABILITY HIDDEN DATA VIA SATELLITE CHANNELS ACCOUNTING LOSSES

*Канд. техн. наук Е.C. Абазина, канд. техн. наук В.Е. Федосеев, Д.В. Леванов Ph.D. E.S. Abazina, Ph.D. V.E. Fedoseev, D.V. Levanov*

*ВКА им. А.Ф. Можайского*

Статья посвящена вопросам обеспечения требуемой достоверности приема дан- ных, передаваемых скрытно в структуре видеопотока по спутниковым радиолиниям с использованием методов цифровой стеганографии. Рассмотрены технологии, при- меняемые в стандарте MPEG-2 для борьбы с ошибками на физическом, канальном и транспортном уровнях модели OSI, предложен алгоритм оценивания достоверно- сти приема данных стегоканалов, организованных в видеопотоке спутниковых ра- диолиний с учетом логики декодирования и восстановления качества видеоданных, передаваемых открыто и используемых для сокрытия.

***Ключевые слова***: достоверность приема, стегоканал, сокрытие данных, видеокон- тейнер, MPEG-2.

The paper is devoted to the issues of ensuring the required reliability of receiving data transmitted covertly in the structure of the video stream over satellite radio lines using digital steganography methods. The technologies used in the MPEG-2 standard to combat errors at the physical, channel and transport levels of the OSI model are considered, an algorithm is proposed to ensure the reliability of receiving data from stegochannels organized in the video stream of satellite radio lines, taking into account the logic of decoding and restoring the quality of video data used as a stegocontainer.

***Keywords***: reception reliability, stegochannel, data concealment, video container, MPEG-2.

## Введение

Анализ тенденций развития современного вооружения и военной техники позволяет в каче- стве одного из наиболее актуальных направлений совершенствования выделить модернизацию си- стем управления. В подавляющем большинстве случаев к управлению средствами вооружения и военной техники предъявляется требование обе- спечения возможности удаленного управления,

а для мобильных средств наличие системы дис- танционного управления является обязательным. При этом успешное выполнение функций любой системой управления определяется качественным состоянием телекоммуникационной инфраструк- туры, которое выражается в достоверности, свое- временности и безопасности связи. В случаях, ког- да объекты управления размещены и выполняют задачи по предназначению на значительном уда- лении от пункта управления, в труднодоступных

районах, в территориальных водах, воздушной или космической сферах, спутниковая связь ста- новится основным родом, используемым для обе- спечения управления. Основной недостаток спут- никовых радиолиний заключается в их высокой разведдоступности, в то время как трафик управ- ления вооружением и военной техникой является критически важным. Устранение указанного не- достатка возможно благодаря применению спосо- бов и методов цифровой стеганографии, позволя- ющих скрыть сам факт передачи информации за счет модификации малозначащих элементов дан- ных, передаваемых открыто, элементами скрыва- емых данных. Модифицируемые данные принято называть стегоконтейнерами. Чем большей избы- точностью обладает стегоконтейнер, тем больший объем информации можно в нем скрыть. Видео- данные имеют наибольшую избыточность. Кро- ме того, в общем объеме телекоммуникационного трафика как сетей общего пользования, так и сетей специального назначения доля видеотрафика воз- растает. Это является определяющим при их вы- боре в качестве стегоконтейнеров. В работах [1–3] установлено, что встраивание данных стегоканала в видеопоток до его компрессии характеризуется большими потерями, однако обладает и большей скрытностью встраивания. Очевидно, что при пе- редаче данных в скрытых каналах, встраиваемых до компрессии стегоконтейнера, потери больше по сравнению с передачей по открытым каналам. Компенсация потерь скрываемых данных на при- емной стороне осуществляется за счет свойства устойчивости к децимации двумерных широкопо- лосных сигнальных конструкций Франка–Уолша и Франка–Крестенсена, используемых при форми- ровании матрицы скрытых каналов [1–3]. Допол- нительные потери в скрытых каналах обусловлены распространением сигналов открытых видеодан- ных в спутниковых радиолиниях, а также перепол- нением буферной памяти коммутационного обору- дования шлюзовых станций спутниковых сетей, приводящим к отказам обработки пакетов. Однако оценивания этих потерь и определения их влия- ния на достоверность приема скрываемых данных в видеопотоках, передаваемых по спутниковым радиолиниям, ранее не осуществлялось. В этой связи задача разработки алгоритма оценивания до- стоверности приема данных стегоканалов, органи- зованных в видеопотоке с учетом потерь в спутни- ковых радиолиниях, является актуальной.

## Обеспечение достоверности приема видеоданных, передаваемых открыто в спутниковых радиолиниях

Организация передачи видеотрафика, пред- ставленного неподвижными видеоданными, пото- ковыми видеоданными, реального и нереального времени, трансляцией телевизионных программ подразумевает в большинстве случаев примене- ние технологий доставки данных в соответствии со стандартами MPEG-2, MPEG-4, а для IP-се- тей — протокола UDP, либо совместное исполь- зование этих технологий. Основными меропри- ятиями обеспечения требуемой достоверности приема видеоданных, передаваемых по открытым спутниковым радиолиниям, являются [1, 2]:

* контроль достоверности принимаемых ви- деоданных на различных уровнях эталонной мо- дели взаимодействия открытых систем по сле- дующим параметрам: отношение сигнал/шум на входе приемника Signal-to-Noise Ratio (SNR), ко- эффициент ошибок модуляции MER (Modulation Error Ratio), коэффициент битовых ошибок BER (Bit Error Ratio), идентификатор потока PID (Program Identifier), коэффициент непрерывно- сти видеопотока CC (Continuity Counter);
* формирование структуры транспортно- го потока MPEG-TS (Transport Stream), которая обеспечивает возможность мультиплексирова- ния элементарных потоков в магистральный и обратные действия для их верного демульти- плексирования на приемной стороне [4];
* применение алгоритмов помехоустойчиво- го кодирования с упреждающим исправлением ошибок Forward Error Correction (FEC).

Использование перечисленных техноло- гий позволяет достичь достоверности приема данных в видеопотоке, передаваемом открыто по спутниковым радиолиниям, значений BER не хуже 10–6–10–12 [5].

## Алгоритм оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных

Достоверность скрываемых данных в сте- гоканале оценивается по показателю коэффици- ента битовых ошибок для скрываемых данных BERстг, требования к значениям которого опреде- ляются видом скрываемых данных: для речевых

сообщений BERстг > 10–3, для команд и сигналов BERстг > 10–9. Реализация оценивания достовер- ности приема данных, скрываемых с примене- нием методов цифровой стеганографии в виде- оданных, передаваемых в спутниковых радио- каналах, предполагает разрешение следующих основных задач:

* + оценивание достоверности скрываемых данных с учетом потерь, вносимых в результате компрессии открытого видеотрафика при встра- ивании, потерь, возникающих при распростра- нении сигнала в среде передачи, а также при об- служивании сетевыми устройствами;
  + порядок мониторинга состояния стего- контейнера на приемной стороне и оповещения стегопередатчика для осуществления адаптив- ного перехода при встраивании скрываемых данных на методы, обеспечивающие большую достоверность.

Разрешение указанных задач требует, с од- ной стороны, разработки алгоритма оценива- ния достоверности приема данных, скрываемых с применением методов цифровой стеганогра- фии в видеоданных, с другой стороны — орга- низации мониторинга качества функциониро- вания спутниковой радиолинии, используемой для передачи видеоданных со встроенным сте- гоканалом. Решение второй задачи может быть получено благодаря применению анализаторов, размещаемых в одной или нескольких точках сети спутниковой связи или интегрированных в терминальное оборудование для оценивания параметров качества обслуживания видеотрафи- ка, в том числе параметров достоверности. Ка- чество принимаемых видеоданных открытого трафика напрямую определяет качество приема скрываемых данных. Таким образом, очевидна прямая корреляционная зависимость между па- раметрами достоверности приема открытых ви- деоданных и параметрами достоверности скры- ваемых в этих данных стегосообщений. Оценка достоверности скрываемых данных формирует- ся в результате сравнения коэффициента бито- вой ошибки стегоданных BERстг с требованиями, предъявляемыми к достоверности конкретного вида сообщений, встраиваемых в стегоконтей- нер. Алгоритм оценивания достоверности прие- ма данных, скрываемых с применением методов цифровой стеганографии в видеоданных, пред- ставлен на рисунке.

Оценивание начинается с измерения значе- ний SNR для сигнала из спутниковой радиоли- нии, несущего информацию открытого видеотра- фика. SNR является безразмерной величиной, равной отношению мощности полезного сигнала к мощности шума на входе приемника, значение которого сравнивается с величиной чувствитель- ности приемника, и составляет суть условия при- ема сигнала из спутниковой радиолинии.

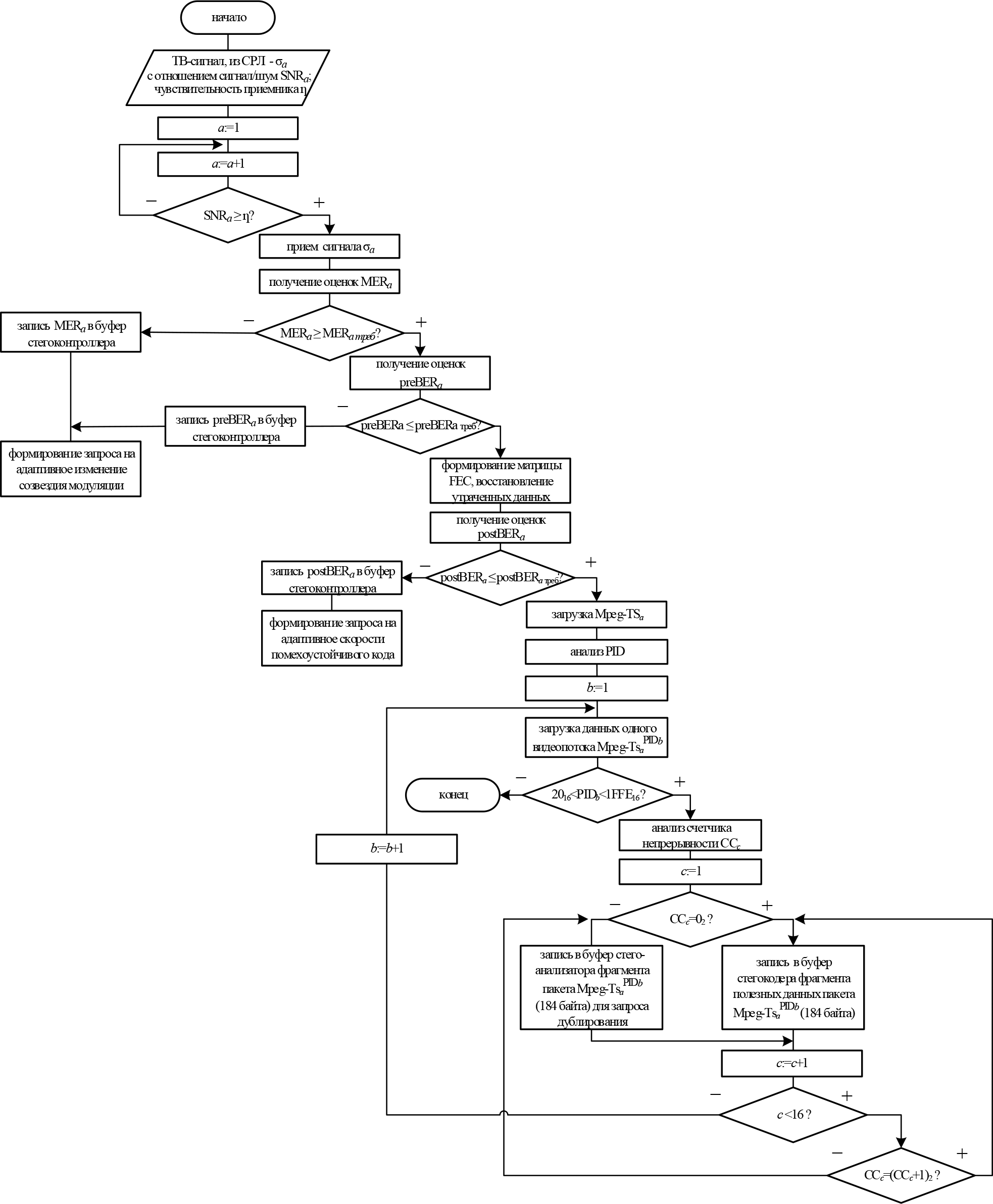
На следующем этапе осуществляется оце- нивание коэффициента MER, отражающего зна- чение величины вектора ошибки [5]. В резуль- тате его сравнения с требуемыми значениями формируется запрос передатчику открытого ви- деотрафика на изменение значности используе- мой модуляции в сторону ее увеличения при хо- рошем состоянии среды передачи, и, наоборот, снижения — при значениях ниже максимально допустимых. Результаты оценки МЕR открытых видеоданных передаются также и стегопередат- чику, который принимает решение об изменении периода используемой двумерной шумоподоб- ной конструкции при формировании стегокана- ла и изменении числа строк матриц видеодан- ных для встраивания дублируемой скрываемой информации [1–3].

Затем выполняется оценивание коэффици-

ента ошибок BER, контролируемого в двух точ- ках — до декодера FEC (preBER) и после него (postBER). Технология FEC предусматривает внесение избыточности путем формирования специальных пакетов FEC. Дополнительная ин- формация (пакеты FEC) передается не постоянно, а лишь при ухудшении качества передаваемого видеопотока. Применение FEC предполагает кли- ент-серверную организацию передатчика и при- емника, использующих анализаторы, называемые контроллерами с функциями защиты от потерь и контроля состояния, которые информируют пе- редающую сторону о возникающих проблемах.

После выполнения указанных процедур

начинается распаковка транспортного потока MPEG-TS, имеющего длину в 188 байт, из кото- рых 4 байта выделяются на заголовок и 184 бай- та — на полезные данные. Каждый пакет перено- сит данные только одного вида. При оценивании потерь в структуре заголовка видеоданных пред- лагаемый алгоритм анализирует лишь значения двух полей заголовка: поле 13-битового иденти- фикатора типа пакета PID (Packet Identifier или



*Рис. Алгоритм оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных*

Program Identification Number) и поле 4-битово- го счетчика непрерывности (СС — Continuity Counter). Идентификатор программ PID указы- вает на принадлежность пакета тому или иному элементарному PES-потоку и позволяет выде- лить в магистральном потоке единственный ви- деоканал. Стегокодер, анализируя PID, принима- ет решение о записи полезной нагрузки каждого из пакетов транспортного потока MPEG-TS, со- держащей скрываемые данные. Для канала с ви- деоданными PID может принимать значения от 20 до 1FFF в 16-тиричной системе счисления.

На следующем этапе осуществляется оце- нивание значений счетчика непрерывности па- кетов транспортного потока СС, являющегося циклическим. Первоначальное значение CC со- ответствует нулю, которое с получением каждо- го нового пакета последовательно увеличивается на единицу до 15, после чего счетчик обнуляет- ся и цикл повторяется. Оценивание числа про- пущенных значений счетчика непрерывности позволяет определить элементы потерянных от- крытых видеоданных, а соответственно и опре- делить какие строки матрицы стегоданных не были получены в результате потерь в открытом транспортном потоке. Извещение передатчика стегоканала о том, какие элементы стегоматри- цы не были получены, позволяет выполнить их дублирование и обеспечить требуемую досто- верность на приемной стороне.

На завершающем этапе выполняется оцени-

вание коэффициента битовых ошибок для скры- ваемых данных BERстг, сведения о котором так- же передаются стегокодеру. При потере не более 20 % восстановление потерянных стегоданных возможно благодаря свойству устойчивости к децимации двумерных шумоподобных сиг- налов Франка–Уолша и Франка–Крестонсона, используемых при формировании стегоканала [3–11]. В противном случае стегокодером прини- мается решение об увеличении периода исполь- зуемой двумерной шумоподобной конструкции для обеспечения требуемых значений показателя коэффициента битовых ошибок для скрываемых данных BERстг не хуже значений, установленных для данного вида трафика.

Таким образом, представленный алгоритм

оценивания достоверности приема данных, скрываемых с применением методов цифровой стеганографии в видеоданных, отличается от из-

вестных учетом потерь открытых видеоданных, выбранных для встраивания, при их передаче по каналам спутниковой сети связи путем оцени- вания достоверности их приема по показателям SNR, MER, PID, CC, BER и BERстг с последую- щим оповещением передающей стороны стего- системы, реализуя адаптивный выбор периода двумерной шумоподобной сигнальной конструк- ции для формирования стегоканала и кратность повторной передачи скрываемых данных.

## Заключение

Вопросы обеспечения достоверности скры- ваемых данных требуют разработки алгоритма оценивания и мониторинга как открытого тра- фика, выступающего в качестве стегоконтейне- ра, так и трафика, передаваемого в стегоканалах. Одна из очевидных задач состоит в интеграции сведений о состоянии стегоданных во множе- ство параметров качества открытого трафика с последующей передачей по служебным каналам открытой связи на передающую сторону для ре- ализации адаптивной подстройки. Представлен- ные предложения формирования канала обрат- ной связи в интересах адаптации стегокодера к условиям передачи являются элементом новиз- ны. Учет особенностей современных техноло- гий, применяемых при восстановлении качества видеоданных, в части, касающейся значений оцениваемых параметров, мониторинг которых предусмотрен при организации транспортных видеотрансляций по стандарту MPEG-2, необхо- дим ввиду их прямой корреляции с достоверно- стью скрываемых данных.

## Литература

1. ISO/IEC 13818-1 (ITU-T H.222.0),

«Information technology — Generic coding of moving pictures and associated audio information: systems». 2002. 15 p.

1. Локшин Б.А. Цифровое вещание. От сту- дии к телезрителю // Учебное пособие. — Мо- сква: Компания Сайрус системс. 2001. 316 с.
2. Цветков К.Ю. Теория оптимальных сис- тем сложных дискретных сигналов и ее прило- жения. — СПб.: ВКА, 2005. 160 с.
3. Абазина Е.С. Формирование стеганогра- фического канала с кодовым уплотнением на ос-

нове двумерных нелинейных сигналов // Вопро- сы радиоэлектроники в сфере техники телевиде- ния. 2015. № 1. С. 15–26.

1. Абазина Е.С. Модель кодера скрытого канала с кодовым уплотнением с использова- нием сигнальных последовательностей Фран- ка–Уолша, Франка–Крестенсона / К.Ю. Цветков, В.Е. Федосеев, В.М. Коровин и др. // Журнал НИИ Радио. 2014. № 2. С. 28–35.
2. Абазина Е.С. Метод скрытой передачи информации с кодовым уплотнением в виде- оданных // Информация и космос. 2014. № 1. С. 33–38.
3. Цветков К.Ю., Ерунов А.А. и др. Алго- ритм кодового уплотнения скрытых каналов с учетом приоритетов абонентов // Известия Ин- ститута инженерной физики. 2016. № 4 (42). С. 25–31.
4. Стеганография, цифровые водяные знаки и стегоанализ: монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин и др. — М.: Вузов- ская книга, 2009. 220 с.
5. Ерунов А.А., Коровин В.М. и др. Вычис- лительная сложность алгоритмов формирова- ния стегоканала с кодовым уплотнением в ви- деопотоке // Труды Военно-космической ака- демии им. А.Ф. Можайского. 2018. Вып. 665. С. 35–45.
6. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: Солон-Пресс, 2009. 272 с.
7. Абазина Е.С., Цветков К.Ю. Концепту- альная модель взаимодействия стегосистем пе- редачи данных в составе эталонной модели вза- имодействия открытых систем // Труды Воен- но-космической академии им. А.Ф. Можайского. 2019. Вып. 668. С. 70–80.

## References

1. ISO/IEC 13818-1 (ITU-T H.222.0),

«Information technology — Generic coding of moving pictures and associated audio information: systems», 2002. 15 p.

1. Lokshin B.A. Digital broadcasting. From the studio to the viewer. — Moscow: Company Sirus systems, 2001. 316 p.
2. Tsvetkov K.Yu. Theory of optimal systems of complex discrete signals and its applications. — Saint-Petersburg: Mozhaisky Military Space Academy, 2005. 160 p.
3. Abazina E.S. Formation of the steganographic channel with a code seal based on two-dimensional nonlinear signals // Radio engineering issues in the field of television technology. № 1. 2015. P. 15–26.
4. Abazina E.S. A model of the hidden channel encoder with a code seal using Frank–Walsh, Frank– Krestenson signal sequences // Journal of the Radio Research Institute. № 2. 2014. P. 28–35.
5. Abazina E.S. Formation of the steganographic channel with a code seal based on two-dimensional nonlinear signals // Information and space. 2014.

№ 1. P. 33–38.

1. Tsvetkov K.Yu., Yerunov A.A., et al. Algorithm of code sealing of hidden channels taking into account the priorities of subscribers // News of Engineering Physics Institute. 2016. № 4 (42). P. 25–31.
2. Steganography, digital watermarks and steganalysis: monograph / A.V. Agranovsky,

A.V. Balakin, V.G. Gribunin et al. — M.: University Book, 2009. 220 p.

1. Erunov A.A., Korovin V.M. et al. Computational complexity of algorithms for the formation of a code-compacted stegocanal in a video stream // Proceedings of the Military Space Academy named after A.F. Mozhaisky. 2018. Issue 665. P. 35–45.
2. Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography. — Moscow: Solon-Press, 2009. 272 p.
3. Abazina E.S., Tsvetkov K.Yu. Conceptual model of interaction of stegosystems of data transmission as part of the reference model of interaction of open systems // Proceedings of the Military Space Academy named after

A.F. Mozhaisky. 2019. Issue 668. P. 70–80.