УДК 621.397.3
DOI 10.18413/2411-3808-2018-45-4-769-781

ВСТРАИВАНИЕ СТЕГАНОГРАФИЧЕСКИХ СООБЩЕНИЙ В ВИДЕОФАЙЛЫ ФОРМАТА MPEG-4

EMBEDDING STEGANOGRAPHIC MESSAGES INTO MPEG-4 VIDEO FILES

С.В. Радаев[1], О.О. Басов[2], К.И. Мясин[1], А.И. Мотиенко[3]
S.V. Radaev[1], O.O. Basov[2], K.I. Myasin[1], A.I. Motienko[3]

[1)] Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации», Россия, 302014, Орёл, ул. Приборостроительная, 35
[2)] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Россия, 197101, Санкт-Петербург, Кронверкский пр., 49
[3)] Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Россия, 199178, Санкт-Петербург, 14 линия, 39

[1)] The Federal state government military educational institution of higher education «The Academy of the Federal Guard Service of the Russian Federation», 35 Priborostroitelnaya St., Orel, 302014, Russia
[2)] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverkskiy prospekt, St. Petersburg, 197101, Russia
[3)] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 39 14-th Linia, St. Petersburg, 199178, Russia

E-mail: radik0782@mail.ru, oobasov@mail.ru, fmmc@mail.ru

Аннотация
В условиях динамичного развития компьютерных технологий наряду с криптографическими методами защиты информации значительный интерес представляют методы стеганографии как альтернативное средство защиты конфиденциальных данных. В статье в качестве стеганографических контейнеров рассмотрены видеофайлы формата MPEG 4, обоснована актуальность такого выбора и практическая значимость. На основе анализа доступного программного обеспечения, реализующего стеганографические алгоритмы, представлены различные варианты встраивания стеганографического сообщения. Исследование возможных вариантов встраивания за счет изменения форматных данных позволило выявить методы, наиболее стойкие к атакам различного рода. На основе таких методов разработаны алгоритмы, обладающие повышенной стеганографической стойкостью. Достоинством предложенных алгоритмов является отсутствие нарушений общей организационной структуры файлового потока при высокой стойкости к классическим методам стегоанализа. Кроме того, в работе показана целесообразность построения комбинированных криптостеганографических систем.

Abstract
Currently, in the conditions of dynamic development of computer technologies along with cryptographic methods the methods of steganography as an alternative means of protecting confidential data are of significant interest. In this connection the analysis of the organization file structures video files of various formats from the point of view of steganographic containers is presented in this paper The article selected MPEG 4 video files as steganographic containers, justified the relevance of this choice and practical significance. Based on the analysis of available steganographic programs, various ways for embedding a steganographic message are presented, the essence of which is to modify the format data. From the presented ways for incorporation of the most preferred and based on them algorithms, which have increased the steganographic strength. The advantage of the proposed algorithms is the absence of violations of the overall organizational structure of the file stream. In addition, the expediency of combinational application of cryptographic and steganographic methods of information protection is actualized.

Ключевые слова: атом, видеофайл, защита информации, конфиденциальная информация, стеганография, стеганографическая стойкость, хэш-код.
Keywords: atom, videofile, information protection, confidential information, steganography, steganographic strength, hash-code.

Введение

При наблюдаемом сегодня росте числа компьютерных атак [https://www.ec-rs.ru/novosti/kiberbezopasnost-2017-2018-tsifryi-faktyi-prognozyi] на инфраструктуру и ресурсы информационного пространства, а также эволюции методов их реализации существующие технические средства защиты инфокоммуникационных систем не всегда способны обеспечить требуемый уровень безопасности информационного обмена. Под угрозой оказываются как персональные данные рядовых пользователей, так и коммерческие секреты крупных корпораций. Особую злободневность данная проблема имеет для полимодальных систем, которые совсем недавно (но весьма активно) начали формироваться в национальном инфокоммуникационном пространстве [Basov, 2017].

В соответствии с [Указ Президента РФ от 09.05.2017 № 203, 2017] важнейшим принципом построения интеллектуальных инфокоммуникационных систем является реализация защиты информации на основе средств криптографии и стеганографии. При этом стеганографические методы защиты информации используются редко и, как правило, в частных целях. Связано это в первую очередь с отсутствием теоретической доказуемости гарантированной стойкости, встроенной с помощью стеганографических систем информации [Рябко, Рябко, 2009]. Вместе с тем в работах [Ажбаев, Ажмухамедов, 2008; Елисеев, 2013] доказывается стеганографическая стойкость, достаточная для широкого класса задач по защите конфиденциальных данных.

Исследования и разработки в области стеганографии становятся все более популярными в связи с широким использованием цифровых форматов мультимедиа. Это обусловлено, во-первых, стремительным развитием вычислительной техники, во-вторых, тем, что ограничения, накладываемые в большинстве стран на криптографические системы (передача ключей, регистрация, лицензирование и др.), не распространяются на стеганографические средства [Постановление Правительства РФ от 16.04.2012 № 313, 2012], в третьих, в качестве контейнера могут передаваться полезные данные, действительно важные для корреспондента (в том числе, использование цифровых водяных знаков).

Прикладные работы в данной области знаний привели к созданию программных продуктов, реализующих стеганографические алгоритмы (например, [http://www.jjtc.com]), онлайн-сервисов, предоставляющих услуги как стеганографии (например, [https://incoherency.co.uk/image-steganography]), так и стеганографического анализа (например, [https://www.backbonesecurity.com/SARC.aspx]).

Широкому распространению данных и аналогичных решений препятствуют как жесткие ограничения на структуру и размер скрываемой информации, нарушение которых приводит к снижению стойкости, так и изначально низкая степень скрытности факта передачи.

Целью настоящей работы является создание стеганографического алгоритма, обладающего большей стойкостью, чем существующие форматные методы.

Текущий уровень развития предметной области

В качестве носителей для скрытой передачи информации чаще всего используются данные мультимедийного характера: изображения, звуковые и видеофайлы различных форматов хранения и передачи [Рябко, 2010]. Такой выбор обусловлен избыточностью получаемых в результате цифровой обработки данных, которая позволяет внедрять («прятать») некоторое количество информации, не оказывающей влияния на различные характеристики исходного носителя.

Ввиду большой информационной емкости и малой исследованности с точки зрения стеганоанализа именно файлы популярных видеоформатов могут быть использованы в качестве стеганографических контейнеров (носителей). К настоящему времени разработано большое количество форматов сжатого видео. Наибольшее распространение получили такие форматы, как MPEG-1, MPEG-2, MPEG-4, DivX, AVI, MOV и некоторые другие.

Изучение открытых источников позволяет оценить примерное соотношение передаваемых и хранимых объектов мультимедийных данных различных видеоформатов, циркулирующих в сети Интернет (рис. 1).

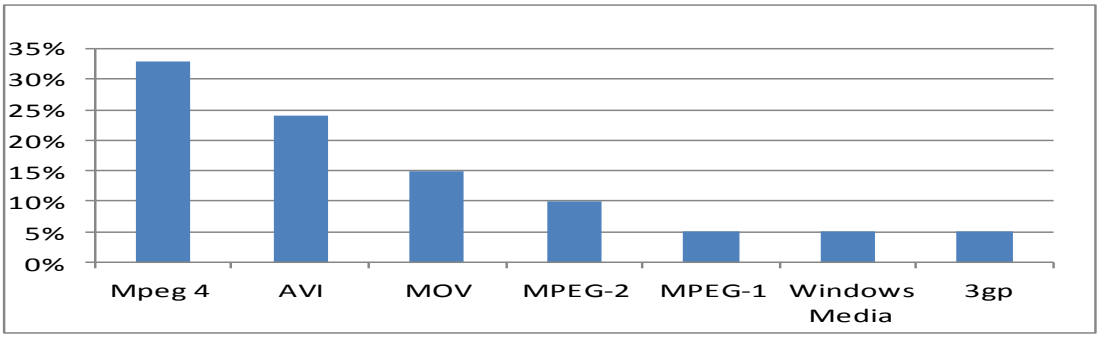

Рис. 1. Соотношение форматов видеофайлов, передаваемых в сети Интернет
Fig. 1. The ratio of video file formats transmitted on the Internet

Анализ показывает, что к наиболее популярным среди пользователей относятся MPEG 4, AVI и MOV. Данное обстоятельство позволяет рассматривать эти форматы как предпочтительные с точки зрения стегоконтейнеров, потому что модифицированный (содержащий скрытую дополнительную информацию) видеофайл в общем потоке таких же видеофайлов не привлекает внимания потенциальных нарушителей (стегоаналитиков), в отличие, например, от редко используемых форматов видео (DV, AVCHD и др.), появление которых вызовет определённый интерес. Это предположение очевидно и закономерно вследствие большого потока передаваемых по сетям связи стегоконтейнеров, из числа которых выбрать модифицированный (содержащий дополнительную информацию) не представляется возможным. В такой ситуации возникает необходимость применения стегоаналитических комплексов, позволяющих осуществлять мониторинг потока видеофайлов в реальном режиме времени. Разработка, проектирование и создание таких автоматизированных комплексов является нетривиальной задачей и оказывается не под силу для отдельных (одиночных) нарушителей. Опираясь на методические рекомендации, утверждённые руководством 8 центра ФСБ России [Рекомендации № 149/54-144 от 21.02.2008], в данном случае рассматриваются нарушители типа H1 и H2, которые располагают только доступными в свободной продаже компонентами средств защиты информации. Следовательно, представляется целесообразным разработать стеганографический алгоритм встраивания конфиденциальной информации в видеофайлы формата MPEG 4 (вследствие его наибольшей распространённости) с целью её защиты от нарушителей типа H1 и H2 при передаче по открытым (незащищённым) каналам связи.

Встраивание может осуществляться как в информационную часть, например, широкоизвестным методом наименьших значащих бит, так и в область служебных полей файла (так называемые форматные методы). Каждый метод обладает своими особенностями: так вложение непосредственно в информационную часть позволяет передать значительный объем данных, пропорциональный исходному размеру контейнера, но обнаруживается методами статистического анализа, а также является хрупким для операций масштабирования, редактирования и конвертации [Дрюченко, 2007]. Форматные методы потенциально стойки к методам статанализа и проведению указанных операций с файлами (при определенных условиях), но позволяют скрытно передать весьма небольшие объемы информации, а также обладают крайне низкой стойкостью к операциям анализа структуры файла.

Модифицированный стегоалгоритм, разрабатываемый в настоящей работе, должен препятствовать решению обеих задач стеганоанализа – выявлению факта передачи и по-

лучению доступа к информации. Для достижения поставленной цели представляется целесообразным использование форматных методов в сочетании с предварительным шифрованием информации.

Экспериментальное исследование существующих стеганографических алгоритмов

С целью выявления особенностей функционирования стеганографических алгоритмов был проведен анализ доступных стеганографических программ DeEgger Embedder [http://deegger-embedder.findmysoft.com] и Masker 7.5 [http://www.softpuls.com/masker], осуществляющих встраивание стеганографической информации в видеофайлы.

Программный продукт DeEgger Embedder поддерживает в качестве контейнеров видеофайлы AVI и MPEG 4. В свою очередь, программный продукт Masker 7.5 обладает большей функциональностью по сравнению с DeEgger Embedder и позволяет скрывать информацию в цифровых данных, представленных в виде изображений, звуковых файлов, видеофайлов различных форматов, исполнительных файлов и др. Кроме того, в программе Masker 7.5 имеется возможность предварительного шифрования встраиваемого стегосообщения при помощи различных алгоритмов криптографического преобразования (Blowfish, Rijndael, CAST5, DES, Serpent, TripleDES, Twofish).

Для определения особенностей работы стеганографических алгоритмов в исследуемых программах проводился следующий эксперимент.

1. В качестве контейнера использовались видеофрагменты в форматах AVI и MPEG 4 продолжительностью до 1 минуты. Скрываемая текстовая информация содержалась в txt-файле размером 32 байта.

2. В анализируемые приложения были загружены исходные данные и на их основе осуществлено встраивание информации в соответствии с описанием к программным продуктам.

3. Группой экспертов осуществлялась визуальная оценка полученных модифицированных видеофайлов. Каких-либо заметных для человеческого глаза искажений видео или звука выявлено не было. Это прогнозируемый результат, учитывая соотношение размеров контейнера и вложения.

4. Детальный анализ структуры файловой организации стегоконтейнеров на предмет выявления модифицированных областей проводился с помощью программного продукта HexWorkshop [http://www.hexworkshop.com]. На рис. 2–4 изображены исходный и модифицированный видеофайлы в формате представления шестнадцатеричного кода.

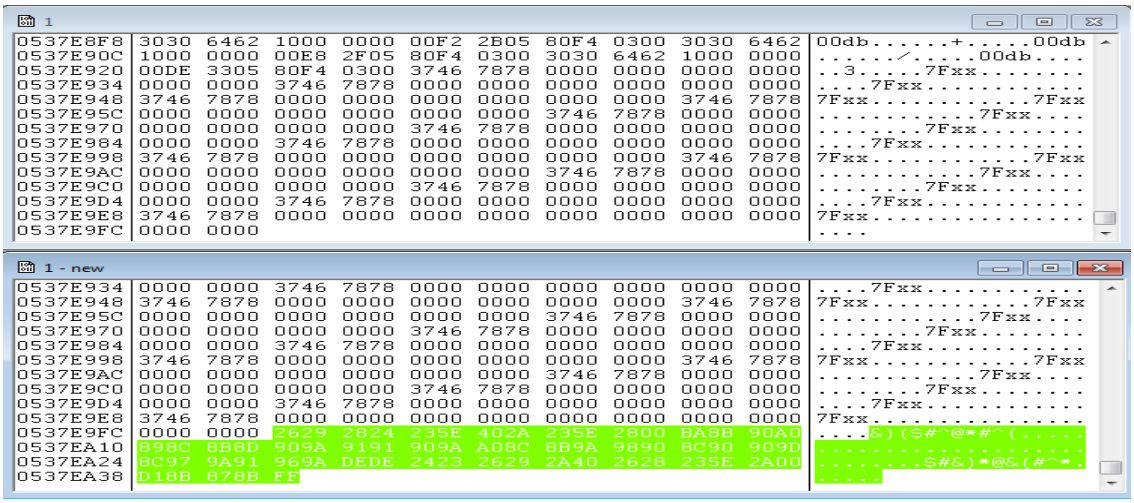

Рис. 2. Сравнение исходного (сверху) и модифицированного (снизу) с помощью программы DeEgger Embedder видеофайлов формата AVI

Fig. 2. Comparison of original (top) and modified (bottom) using the program DeEgger Embedder video files of the AVI format

Представленные на рис. 2–4 структуры пустых (в верхней части) и заполненных (в нижней части) контейнеров свидетельствуют об увеличении объема файла за счет появления новых областей адресного пространства (выделено заливкой).

Причем вставка дополнительной информации осуществляется в конце файла – сравнительный анализ байтовых структур указанных файлов и соответствующих им модифицированных файлов показывает наличие дополнительной информации после маркеров окончания видеофайлов (в нижних частях рассматриваемых рисунков).

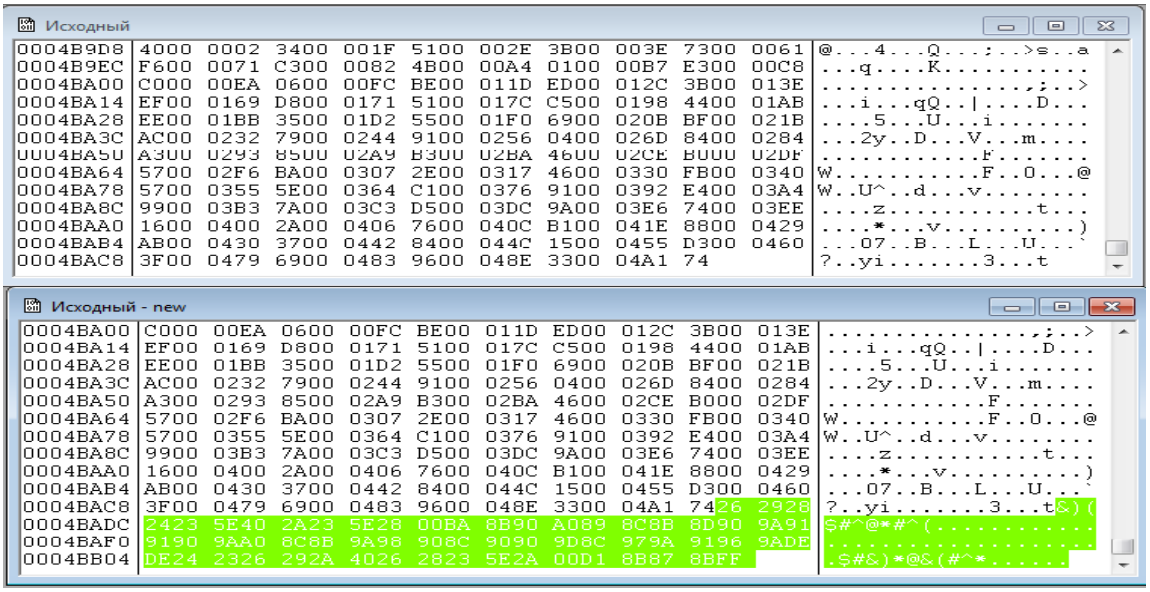

Рис. 3. Сравнение исходного (сверху) и модифицированного (снизу) с помощью программы DeEgger Embedder видеофайлов формата MPEG 4

Fig. 3. Comparison of original (top) and modified (bottom) using the program DeEgger Embedder video files of the AVI format MPEG 4

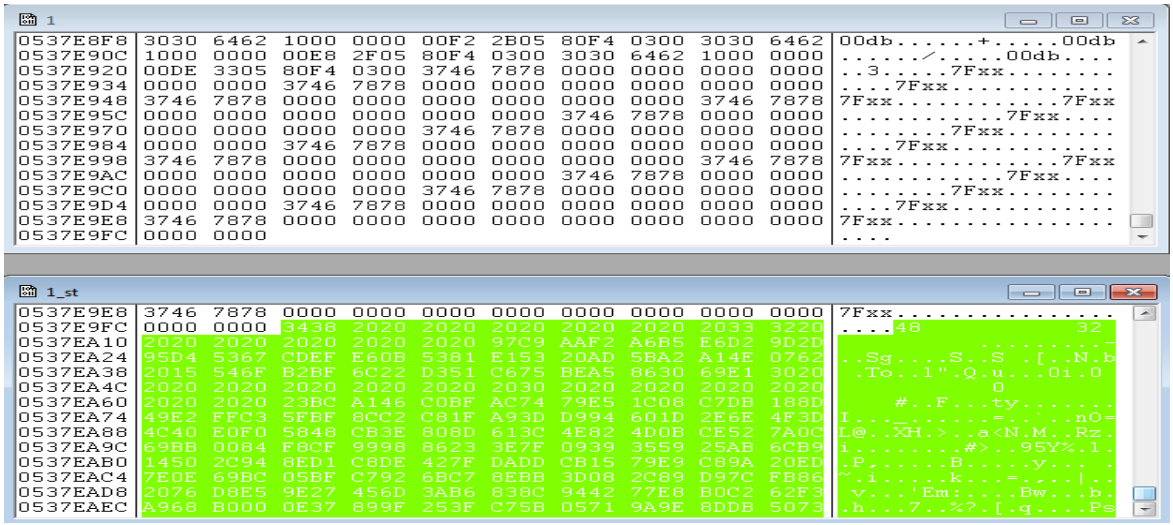

Рис. 4. Сравнение исходного (сверху) и модифицированного (снизу) с помощью программы *Masker 7.5* видеофайлов формата avi, представленных в редакторе файлов Hexworkshop

Fig. 4. Comparison of the original (top) and modified (bottom) using the program Masker 7.5 avi video files presented in the file editor Hexworkshop

Из представленных результатов следует, что встраивание дополнительной информации в обеих стеганографических реализациях осуществляется форматным методом, а именно способом дописывания данных в конец файла. Следует отметить, что, несмотря на одинаковый размер встраиваемых стегосообщений, объём встроенных данных

с помощью различных программ различается. Это связано в первую очередь с реализацией предварительного шифрования и, как следствие, с добавлением дополнительной информации о параметрах используемого криптографического преобразования. В качестве достоинства рассматриваемых алгоритмов можно отметить простоту реализации, однако ключевым недостатком является крайне низкая стеганографическая стойкость. Если значения байт окончания файла отличны от типовых значений, декларированных в описании формата, можно утверждать о решении первой задачи стеганоанализа. Все адресное пространство между окончанием видео и концом файла содержит стеганографическое вложение.

Другим примером форматного метода является внедрение стегосообщения в межкадровый интервал [Радаев, Кирюхин, Иванов, 2010]. Основными достоинствами этого метода являются простота реализации и практически полное отсутствие внесения искажений в видеопоток. Межкадровый интервал – это область, расположенная в потоке между группами кадров и используемая кодеками для передачи своей, служебной информации. Межкадровый интервал не имеет характерных особенностей построения и не выделяется в общей структуре видеопотока, что оказывает положительное воздействие на стеганографическую стойкость встроенного сообщения [Жиляков, Черноморец, Болгова, Гахова, 2014]. Это связано с тем, что заполняется межкадровый интервал псевдослучайной последовательностью. Однако в качестве недостатка рассматриваемого способа следует отметить небольшой объём встраиваемых данных вследствие ограниченности длины межкадрового интервала, которая не превышает 1024 бита. Данный метод пригоден для передачи цифровых водяных знаков и текстовых сообщений длиной до 1000 знаков (например, электронной подписи).

Для определения полей видеофайла, позволяющих осуществить вложение наиболее скрытно, требуется провести анализ организации структуры видеофайлов формата MPEG 4.

Анализ организации структуры видеофайлов формата MPEG 4

Структура файла *MPEG 4* состоит (рис. 5) из дерева блоков, называемых атомами.

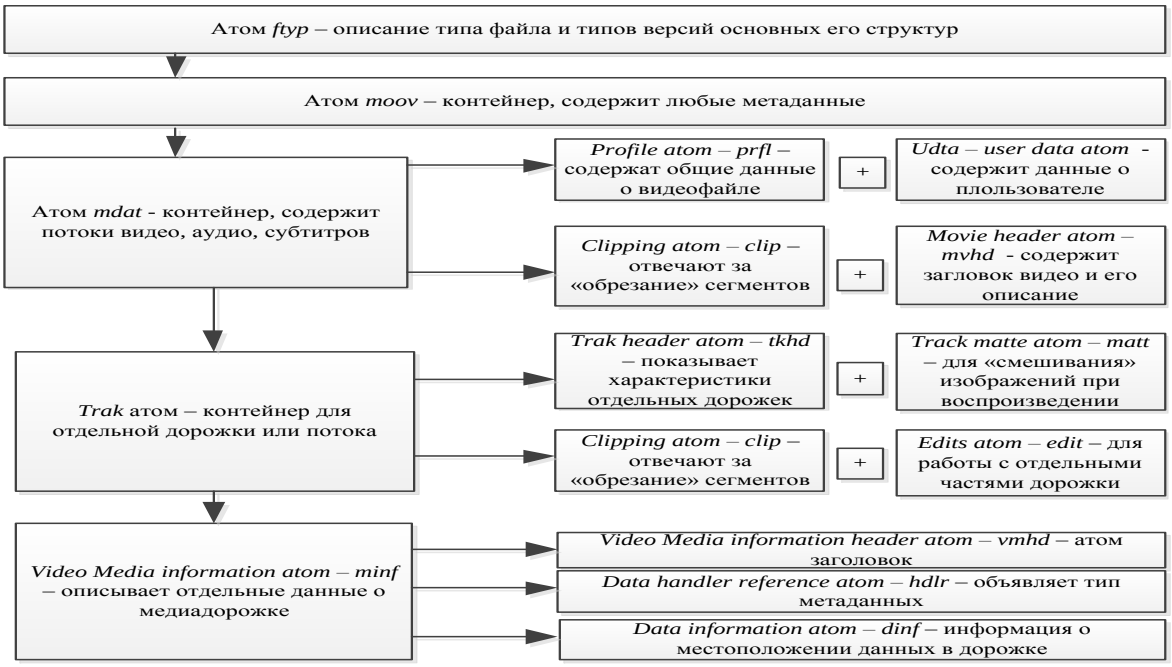

Рис. 5. Типовая структура организации файлового формата MPEG 4
Fig. 5. A typical structure of MPEG 4 file format

Атомы могут содержать какие-либо данные или являться контейнерами для других атомов. Атомы имеют иерархическую фиксированную структуру типов. Синтаксически атомы устроены в соответствии с таблицей.

Таблица
Table

Синтаксическая структура атома
Syntactic structure of the atom

Номера байтов	Назначение
0…3	Размер атома в байтах (включая эти 4 байта). Ограничивается 4 гигабайтами.
4…7	Название (имя) атома (6674 7970 (hex) или ftyp, 6D64 6174 (hex) или mdat, 6D6F 6F76 (hex) или moov и др.)
8…	Содержимое (тело, данные) атома

Атом «ftyp» всегда располагается первым в файле формата MPEG 4 и содержит тип этого файла и типы версий основных структур файла. Неформатные данные видеофайла «вкладываются» в атом «moov» (рис. 6), который содержит информацию об аудио и видеопотоках. Данные атома «moov», начинающиеся с 8-го байта в атоме, имеют древовидную структуру, состоящую из блоков такого же формата, что и атом (т. е. 4 байта – размер блока, следующие 4 байта – имя блока, с 8-го байта – данные блока данных). Кроме того, данный атом напрямую взаимодействует с атомом mdat, который содержит в себе дополнительные, служебные или метаданные (потоки аудио, видео, субтитры), необходимые для воспроизведения видеофрагмента.

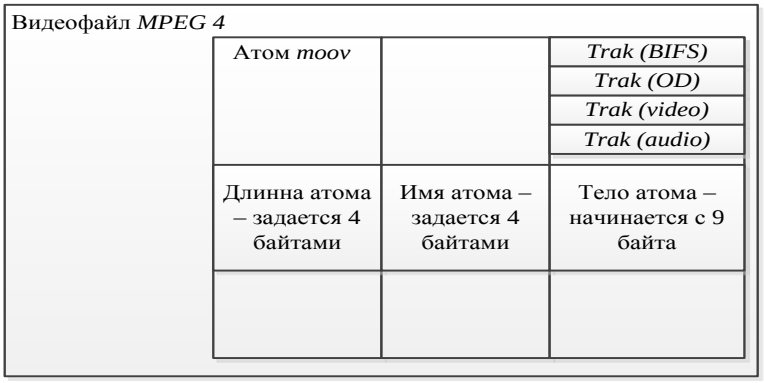

Рис. 6. Схема атома moov
Fig. 6. Scheme of moov atom

В ходе исследования было установлено, что не все атомы форматной части видеофайла являются пригодными для встраивания в них дополнительной информации, так как в некоторых случаях их модификация критично сказывается на работе кодека. Однако после проведения серии экспериментов были определены наиболее подходящие для модификации атомы.

Эксперимент проводился для следующих исходных данных:

– видеофайл-контейнер формата MPEG 4 (длительностью 31 секунда, размером 309977 байт) (рис. 7);

– 32-байтовая последовательность осмысленного текста «Eto_vstroennoe_stegosoobshenie!!» в качестве стегосообщения для упрощения поиска места вложения в структуре файла.

Небольшие размеры опытных образцов позволили сократить временные затраты на проведение экспериментов. Аналогичные результаты могут быть получены при произвольном соотношении размеров контейнера и вложения.

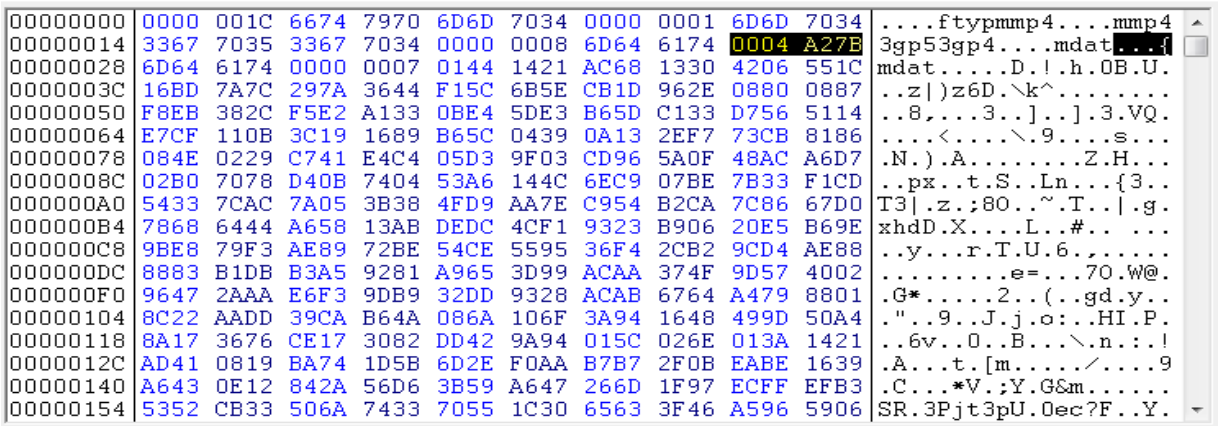

Рис. 7. Представление части исходного видеофайла в редакторе файлов Hex Workshop v6.8 в шестнадцатеричном формате

Fig. 7. Representation of part of the original video file in Hex Workshop v6.8 file editor

В первой серии экспериментов осуществлялось встраивание информации в конец первого атома mdat (6D64 6174 (hex)). Для этого его исходный размер (00000008 (hex)) был предварительно увеличен на величину встраиваемого стегосообщения 00000020 (hex) (в итоге размер составил 00000028 (hex)). Затем после атома mdat (6D64 6174 (hex)) был добавлен текст стегосообщения. Результат встраивания изображен на рис. 8 (встроенное сообщение отмечено черным цветом).

При воспроизведении модифицированного видеофрагмента появились демаскирующие признаки, выразившиеся в искажении изображения и отсутствии звукового сопровождения. Анализ характера искажений выходит за рамки данной работы, однако можно полагать, что между модификацией атома mdat и спецификой искажений есть зависимость, позволяющая однозначно идентифицировать факт вложения дополнительной информации.

Следует отметить, что встраивание осуществлялось простейшим способом, то есть без применения к стегосообщению процедуры сжатия и предварительного шифрования. Поэтому встроенное сообщение отображается в явном виде (см. рис. 8). Тем не менее описанный способ встраивания непригоден ввиду невозможности воспроизведения модифицированного видеофрагмента.

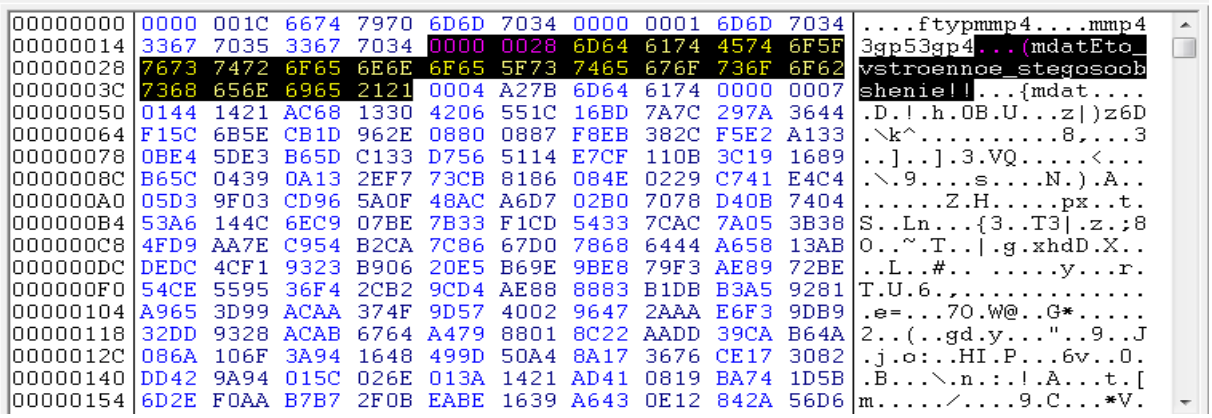

Рис. 8. Представление части модифицированного видеофайла в редакторе файлов Hex Workshop v6.8 в шестнадцатеричном формате

Fig. 8. Representation of part of a modified video file in Hex Workshop v6.8 file editor

В следующей серии экспериментов в структуру видеофайла добавлялся дополнительный атом meta, содержащий метаданные (meta – 6D65 7461 (hex)). В соответствии с синтаксической структурой (согласно таблице) задавался его размер (40 байт = 8 (длина

и название) + 32 (стегосообщение)). Данный искусственно созданный атом, содержащий стегосообщение, размещался непосредственно перед первым атомом mdat (6D64 6174 (hex)). Результат встраивания представлен на рис. 9.

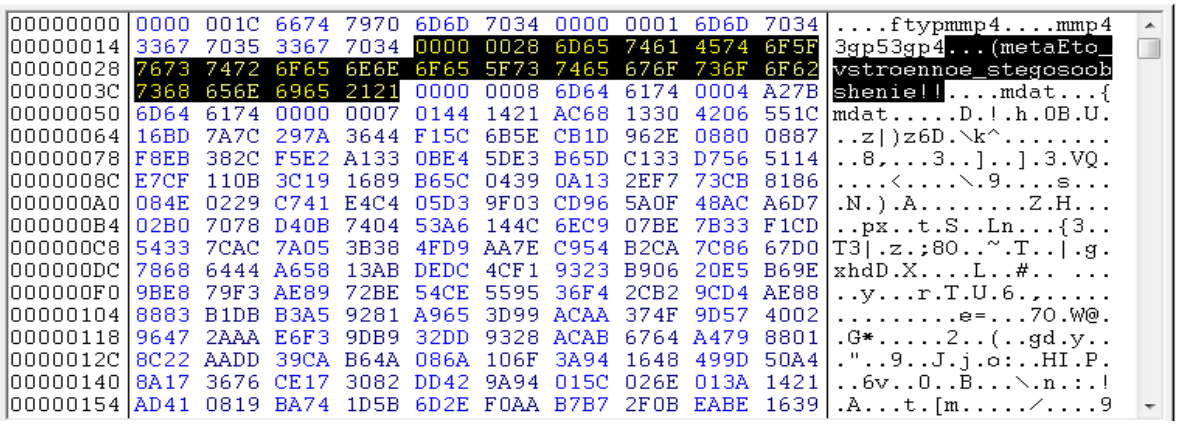

Рис. 9. Представление части модифицированного видеофайла в редакторе файлов Hex Workshop v6.8 в шестнадцатеричном формате
Fig. 9. Representation of part of a modified video file in Hex Workshop v6.8 file editor

Несмотря на то, что структура атома mdat (6D64 6174 (hex)) не была модифицирована (как в первом случае), тем не менее при воспроизведении видеофрагмента появились демаскирующие признаки, выразившиеся в искажении изображения в нижней части кадров и отсутствии звукового сопровождения. Значит, предложенный способ встраивания также не имеет смысла реализовывать.

В третьей серии экспериментов также создавался дополнительный атом meta (6D65 7461 (hex)), и располагался он между двумя обязательными атомами mdat (6D64 6174 (hex)) таким образом, чтобы не нарушить синтаксическую структуру (согласно таблице). Результат встраивания представлен на рис. 10.

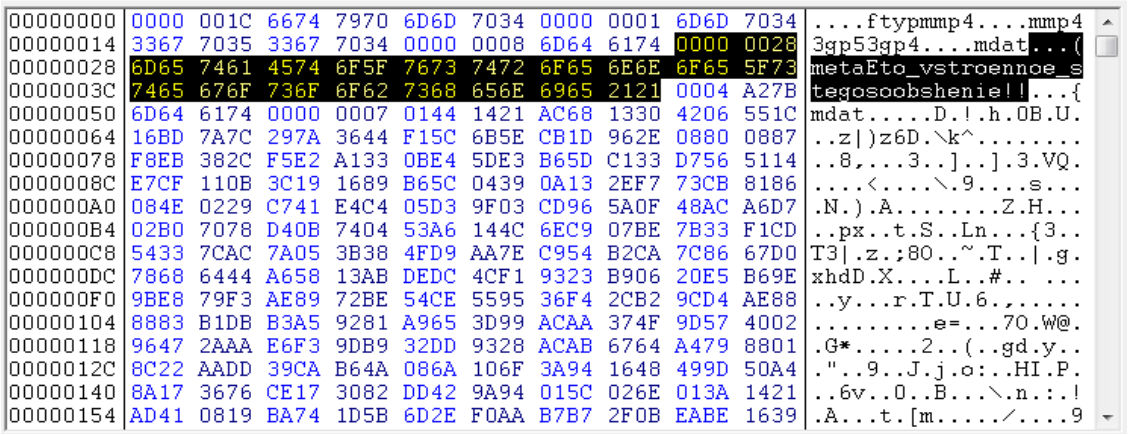

Рис. 10. Представление части модифицированного видеофайла в редакторе файлов Hex Workshop v6.8 в шестнадцатеричном формате
Fig. 10. Representation of part of a modified video file in Hex Workshop v6.8 file editor

Как и в предыдущих двух экспериментах при воспроизведении видеофрагмента появились демаскирующие признаки, выразившиеся в искажении кадров изображения и отсутствии звукового сопровождения.

На основе проведенных экспериментов сделан вывод, что дополнительный атом meta (6D65 7461 (hex)) следует добавлять после двух обязательных атомов mdat (6D64 6174 (hex)). Результат встраивания представлен на рис. 11.

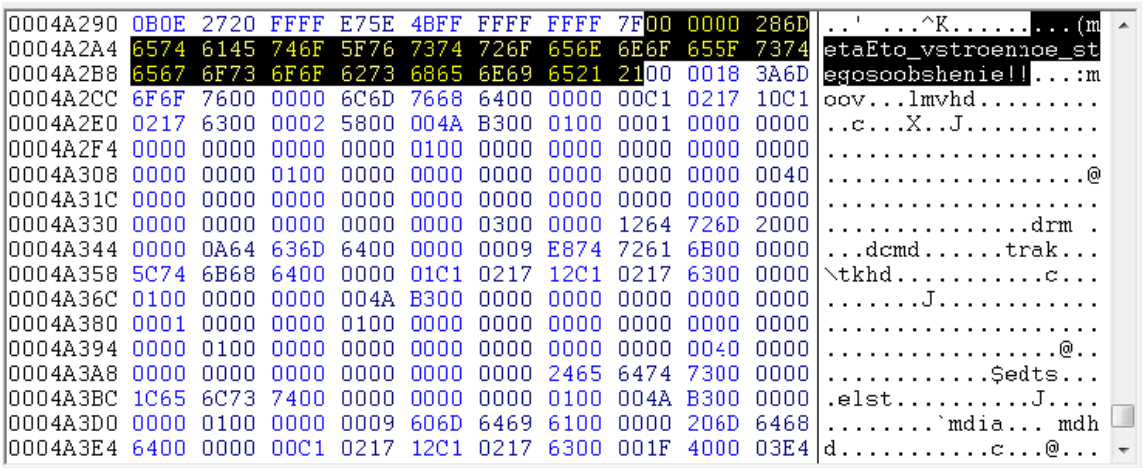

Рис. 11. Представление части модифицированного видеофайла в редакторе файлов Hex Workshop v6.8 в шестнадцатеричном формате

Fig. 11. Representation of part of a modified video file in Hex Workshop v6.8 file editor

Для реализации данного способа встраивания следует найти окончание второго атома mdat (6D64 6174 (hex)), для чего в редакторе файлов Hex Workshop определить его размер и переместиться от текущей позиции на соответствующую величину. На рис. 7 байты, отвечающие за длину атома, выделены черным цветом и имеют величину 0004 A27B (hex) или 303739 байт (dec). Затем следует создать атом meta (6D65 7461 (hex)) с соответствующей организацией файловой структуры и встроить в него стегосообщение. При воспроизведении видеофрагмента заметных визуальных и звуковых искажений членами экспертной группы выявлено не было. Таким образом, можно сделать вывод, что предложенный способ встраивания является приемлемым.

Однако анализ файловых структур различных видеофайлов формата MPEG 4 выявил, что в большинстве образцов видеофайлов дополнительный атом meta (6D65 7461 (hex)) отсутствует. Следовательно, его наличие может вызвать повышенный интерес с точки зрения пассивного стегоаналитика.

В этой связи более предпочтительным представляется встраивание стегосообщения путём модификации имеющихся обязательных атомов, а именно способ встраивания стегосообщения в тело (конец данных) второго атома mdat (6D64 6174 (hex)) перед атомом moov (6D6F 6F76 (hex)). Результат встраивания согласно указанному способу представлен на рис. 12.

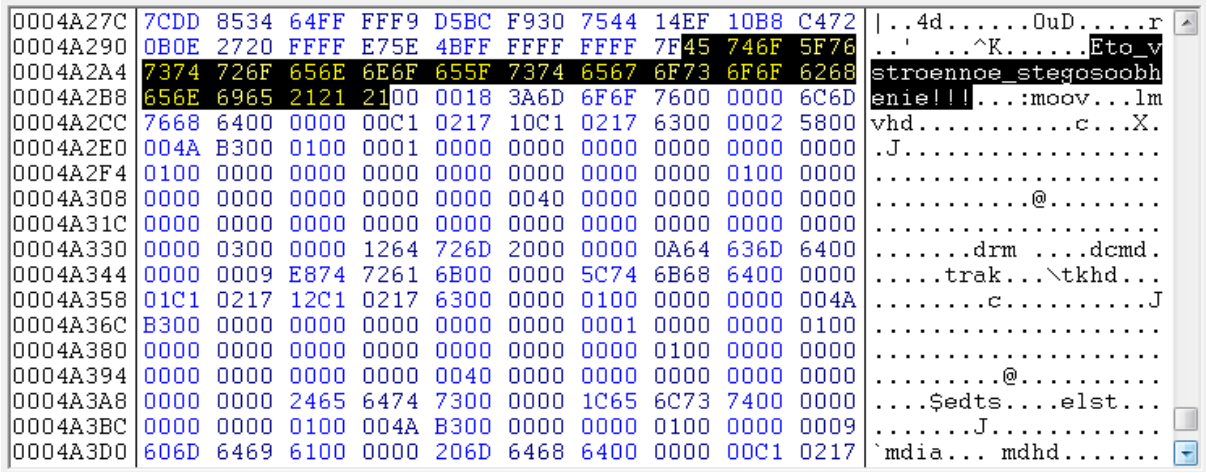

Рис. 12. Представление части модифицированного видеофайла в редакторе файлов Hex Workshop v6.8 в шестнадцатеричном формате

Fig. 12. Representation of part of a modified video file in Hex Workshop v6.8 file editor

Для реализации предложенного способа необходимо выполнить следующее:

– найти окончание второго атома mdat (6D64 6174 (hex)), для чего определить его размер в редакторе файлов Hex Workshop. На рис. 7 байты, отвечающие за длину атома, выделены чёрным цветом и имеют величину 0004 A27B (hex) или 303739 байт (dec);

– увеличить действительный размер атома на величину встраиваемого сообщения (на 32 байта). Результирующий размер будет равен 0004A29B (hex) или 303771 (dec);

– переместиться от текущей позиции (от первого байта, отвечающего за длину атома) на величину 0004A27B (hex);

– встроить предварительно зашифрованное стегосообщение.

Из рис. 11 видно, что встроенное стегосообщение располагается в конце атома mdat (6D64 6174 (hex)) непосредственно перед атомом moov. При воспроизведении модифицированного видеофрагмента визуальных и звуковых искажений замечено не было. За счет шифрования обнаружить текстовое вложение простым анализом структуры файла невозможно. К методам статистического стеганоанализа предлагаемый способ стоек ввиду наследования родовых качеств форматных методов встраивания. Предварительно зашифрованное вложение в конце атома mdat будет выглядеть для нарушителя как специфические метаданные, оставленные источником видеофайла (программой монтажа, видеокамерой). Таким образом, можно сделать вывод, что предложенный способ встраивания является наиболее предпочтительным с точки зрения оптимального соотношения объёма встраиваемого стегосообщения и стеганографической стойкости.

Кроме того, при помощи предложенного способа в качестве встраиваемого сообщения возможно использовать как контрольную сумму (хэш-код) от встроенного неформатным методом сообщения, так и само стегосообщение. В первом случае в результате информационного взаимодействия будет обеспечиваться не только скрытая передача конфиденциальной информации, но и существует возможность проверки целостности стеганографического сообщения и контейнера путём сравнения извлечённого хэш-кода и вычисленного хэш-кода от переданного стегосообщения [Радаев, Орлов, Басов, 2017].

Для повышения защищённости передаваемой информации рекомендуется предварительно (перед встраиванием в видеофайл) сжать встраиваемое стегосообщение, зашифровать его одним из известных и надёжных криптографических алгоритмов, например, [ГОСТ Р 34.12–2015] и подписать его [ГОСТ Р 34.10–2012]. Полученная при этом криптостеганографическая система позволяет скрытно и надежно передавать конфиденциальную информацию. Сложность получения доступа к содержанию информации в этом случае определяется криптографической стойкостью применяемого алгоритма шифрования.

Направлением дальнейших исследований является встраивание стегосообщений в изображения (кадры), выделенные из видеопотока, причём, изображения предварительно подразделяются на классы субполосных компонент, что, как ожидается, позволит повысить стеганографическую стойкость встроенного сообщения [Жиляков, Черноморец, Болгова, 2016].

Заключение

В настоящее время в современной западной литературе заметно сократилось количество публикаций в области стеганографии. Из этого можно сделать вывод о перспективности стеганографических методов с точки зрения сохранения в тайне уникальных идей и последующей реализации алгоритмов. Кроме того, в большинстве развитых стран на криптографические системы накладываются ограничения, а на современные системы маскирования и стеганографии таких ограничений нет, что позволяет использовать стеганографические методы для защиты личных данных пользователей интеллектуальных инфокоммуникационных систем. Тем не менее стоит иметь в виду, что ответственность за выбор надёжных способов и алгоритмов гарантированной защиты информации возлагается на пользователя, который должен учитывать всевозможные риски при передаче конфиденциальной информации, вплоть до её умышленного уничтожения.

Современная стеганография является достаточно мощным инструментом сохранения конфиденциальности информации, а её применение давно признано эффективным средством защиты не только авторских прав, но и любой информации, которая относится

к интеллектуальной собственности. Следует отметить, что особенно эффективно комбинированное использование стеганографии и криптографии. В этом случае осуществляется двухуровневая защита передаваемых данных [Шелковый, Миронов, Басов, 2018], взлом которой возможен будет только при компрометации ключевых данных [Шнайер, 2016].

Работа выполнена при финансовой поддержке фонда РФФИ (проект № 18-07-00380).

Список литературы
References

1. Ажбаев Т.Г., Ажмухамедов И.М. 2008. Анализ стойкости современных стеганографических алгоритмов. Вестник АГТУ. Серия «Информационная безопасность». Астрахань, Астраханский государственный технический университет. 1(42): 56–61.

Azhbaev T.G., Azhmukhamedov I.M. 2008. The analysis of resistance of modern steganos algorithms. Vestnik AGTU. Astrakhan, Astrakhan State technical University. 1(42): 56–61.

2. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. Дата введения 01.01.2016.

GOST R 34.12–2015. Information technology. Cryptographic protection of information. Block ciphers. Date of introduction 01.01.2016. (in Russian).

3. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Дата введения 01.07.2012.

GOST R 34.10–2012. Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature. Date of introduction 01.07.2012.

4. Дрюченко М.А. 2007. Алгоритмы выявления стеганографического скрытия в JPEG-файлах. Вестник ВГУ. Серия «Системный анализ и информационные технологии». Воронеж, Воронежский государственный университет. 1: 21–30.

Dryuchenko M.A. 2007. Detection algotithms for steganographic hiding in jpeg files. Vestnik VGU. Voronezh, Voronezh State University. 1: 21–30.

5. Елисеев А.С. 2013. Исследование и разработка методов и алгоритмов стеганографического анализа отдельных контейнеров и их связанных наборов. Дис. канд. техн. Наук. Ростов-на-Дону, 173.

Eliseev A.S. 2013. Issledovanie i razrabotka metodov i algoritmov steganograficheskogo analiza otdel'nyh kontejnerov i ih svyazannyh naborov. dis. kand. tekhn. Sciences. Rostov-na-Donu, 173. (in Russian)

6. Жиляков Е.Г., Черноморец А.А., Болгова Е.В., Гахова Н.Н. 2014. Исследование устойчивости стеганографии в изображениях. Научные ведомости Белгородского государственного университета. Серия «Экономика. Информатика». 1(172): 168–174.

Zhilyakov E.G., Chernomorets A.A., Bolgova E.V., Gakhova N.N. 2014. Study of steganography stability in images. Belgorod State University Scientific Bulletin. Economics Information technologies. 1(172): 168–174.

7. Жиляков Е.Г., Черноморец А.А., Болгова Е.В. 2016. Об информационных подобластях пространственных частот изображений. Научные ведомости Белгородского государственного университета. Серия «Экономика. Информатика». 23(244): 87–92.

Zhiljakov E.G., Chernomorec A.A., Bolgova E.V. 2016. On information subregions of spatial frequencies of images. Belgorod State University Scientific Bulletin. Economics Information technologies. 23(244): 87–92.

8. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», М., 2012.

Decree of government of the Russia Federation No 313, 16.04.2012 « Ob utverzhdenii Polozheniya o licenzirovanii deyatel'nosti po razrabotke, proizvodstvu, rasprostraneniyu shifroval'nyh (kriptograficheskih) sredstv, informacionnyh sistem i telekommunikacionnyh sistem, zashchishchennyh s ispol'zovaniem shifroval'nyh (kriptograficheskih) sredstv, vypolneniyu rabot, okazaniyu uslug v oblasti shifrovaniya informacii, tekhnicheskomu obsluzhivaniyu shifroval'nyh (kriptograficheskih) sredstv, informacionnyh sistem i telekommunikacionnyh sistem, zashchishchennyh s ispol'zovaniem shifroval'nyh (kriptograficheskih) sredstv

(za isklyucheniem sluchaya, esli tekhnicheskoe obsluzhivanie shifroval'nyh (kriptograficheskih) sredstv, informacionnyh sistem i telekommunikacionnyh sistem, zashchishchennyh s ispol'zovaniem shifroval'nyh (kriptograficheskih) sredstv, osushchestvlyaetsya dlya obespecheniya sobstvennyh nuzhd yuridicheskogo lica ili individual'nogo predprinimatelya)», M., 2012. (in Russian).

9. Радаев С.В., Кирюхин Д.А., Иванов И.В. 2010. Разработка алгоритма встраивания цифрового водяного знака в файлы формата MPEG-4. Известия Орёл ГТУ. 1/57(584): 13–17.

Radaev S.V., Kiryuhin D.A., Ivanov I.V. 2010. Development of an embedding algorithm of a digital watermark into MPEG 4 files. Izvestiya Oryol GTU. 1/57(584): 13–17.

10. Радаев С.В., Орлов Д.В., Басов О.О. 2017. Комбинированный стеганографический алгоритм встраивания конфиденциальной информации в цифровые изображения формата JPEG. Научные ведомости Белгородского государственного университета. Серия «Экономика. Информатика». 23(272). 44: 185–192.

Radaev S.V., Orlov D.V., Basov O.O., 2017. Steganographic combination algorithm of embedding the confidential information into the jpeg digital images. Belgorod State University Scientific Bulletin. Economics Information technologies. 23(272): 185–192.

11. Рябко Б.Я., Рябко Д.Б. 2009. Асимптотически оптимальные совершенные стеганографические системы. Пробл. передачи информ. 45(2): 119-126.

Ryabko, B.I., Ryabko D.B. 2009. Asymptotically optimal perfect steganographic systems. Problems of information transfer. 45(2): 119-126.

12. Рябко Б.Я., Фионов А.Н. 2010. Основы современной криптографии и стеганографии. М.: Горячая линия Телеком, 232.

Ryabko B.I., Phionov A.N. 2010. Basics of modern cryptography and steganography. M.: Hot line Telecom, 232.

13. Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», М., 2017.

Ukaz Prezidenta RF ot 09.05.2017 № 203 «O strategii razvitiya informacionnogo obshchestva v Rossijskoj Federacii na 2017–2030 gody», M., 2017. (in Russian).

14. ФСБ РФ. 2008. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Методические рекомендации № 149/54-144 от 21.02.2008.

FSS RF. 2008 Methodical recommendations for using of cryptocredits the security of personal data during their processing in personal data information systems with the use of automation. Recommendation № 149/54-144 from 21.02.2008.

15. Шелковый Д.В., Миронов О.В., Басов О.О., 2018. Моделирование потоков данных реального времени в защищенных корпоративных мультисервисных сетях связи на основе детерминированного сетевого исчисления. Научные ведомости Белгородского государственного университета. Серия «Экономика. Информатика». 45(3): 584-593.

Shelkovyi D.V., Mironov O.V., Basov O.O. Simulation of real-time data flows in protected corporate multiservice communication networks based on deterministic network calculus. Belgorod State University Scientific Bulletin. Economics Information technologies. 45(3): 584-593.

16. Шнайер Б., 2016. Прикладная криптография, 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С.

17. Schneier B., 2016. Applied cryptography, 2nd edition. Protocols, algorithms and source texts in C.

18. Basov O.O. 2017. Principles of constructing polymodal infocommunication systems for information space user service. 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017), 70–75.

19. https://www.ec-rs.ru/novosti/kiberbezopasnost-2017-2018-tsifryi-faktyi-prognozyi.

20. http://www.jjtc.com.

21. https://incoherency.co.uk/image-steganography.

22. https://www.backbonesecurity.com/SARC.aspx.

23. https://www.azfiles.ru/extension/mov.html.

24. http://deegger-embedder.findmysoft.com.

25. http://www.softpuls.com/masker.

26. http://www.hexworkshop.com.

27. https://www.ec-rs.ru/novosti/kiberbezopasnost-2017-2018-tsifryi-faktyi-prognozyi.