6. *Сикарев А. А.* Оптимальный прием дискретных сообщений / А. А. Сикарев, А. И. Фалько. — М.: Связь, 1978. — 328 с.

7. *Каретников В. В.* Система мониторинга плавучей навигационной обстановки на внутренних водных путях России // В. В. Каретников, А. А. Сикарев, Г. Б. Чистяков [и др.] // Морская радиоэлектроника. — 2013. — № 3 (45). — С. 34–35.

8. *Волков Р. В.* К вопросу определения зоны действия системы мониторинга средств навигационного ограждения / Р. В. Волков, В. В. Каретников, А. П. Яснов // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2014. — № 3 (25). — С. 24–27.

9. *Финк Л. М.* Теория передачи дискретных сообщений / Л. М. Финк. — Изд. 2-е. — М.: Сов. радио, 1970. — 728 с.

10. *Каретников В. В.* Совершенствование систем управления судами с использованием автоматизированных идентификационных систем на внутренних водных путях / В. В. Каретников, И. А. Сикарев // Журнал университета водных коммуникаций. — 2010. — № 3. — С. 93–96.

11. *Волков А. Б.* Алгоритмы определения дальности и радиуса зоны действия автоматической информационной системы, работающей в условиях сложной помеховой обстановки / А. Б. Волков, В. В. Каретников, И. А. Сикарев // Мехатроника, автоматизация, управление. — 2009. — № 10. — С. 62–64.

**УДК 004.056.5**

**М. Р. Бухарметов,**
асп.;

**Э. П. Теплов,**
д-р полит. наук, проф.

# ЗАЩИТА ГРАФИЧЕСКИХ ДОКУМЕНТОВ ПУТЕМ ВСТРАИВАНИЯ ПОЛУХРУПКИХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ НА ОСНОВЕ МОДУЛЯЦИИ ЯРКОСТИ

# GRAPHIC DOCUMENTS PROTECTION BY EMBEDDING A DIGITAL WATERMARK BASED BRIGHTNESS MODULATION

*В статье описывается робастный метод защиты графических документов на основе алгоритма модуляции яркости. Защита осуществляется путем встраивания цифрового водяного знака в исходное незащищенное изображение. Приведенный алгоритм позволяет одновременно обеспечивать скрытое встраивание произвольной информационной последовательности заданного объёма и аутентификацию графического документа. Данный метод устойчив к геометрическим атакам на стегоконтейнер, таким как кадрирование, повороты, кратные 90 °, частичное удаление информации из области изображения-контейнера. Дублирование встраиваемой скрытой информации на основе псевдослучайного распределения блоков графического документа усиливает защиту цифрового водяного знака от внешних геометрических воздействий на стегоконтейнер. В то же время поблочная проверка информационной последовательности путем нахождения одинаковых элементов ключа позволяет выявлять возможные области модификации изображения.*

*This article describes a robust method of protection of graphic documents based on the brightness modulation algorithm. Protection is carried out by inserting the digital watermark in the original unprotected images. The algorithm allows to simultaneously provide covert insertion of an arbitrary sequence of a given volume of information and graphic document authentication. This method is resistant to geometric attacks on stegocontainer, such as cropping, rotation, multiples of 90 degrees, the partial removal of information from the image container. Duplicating of embeddable hidden information, on the basis of pseudorandom distribution of units of the graphic document, strengthens protection of digital watermark against external geometrical influences on a stegocontainer. At the same time block-check of information sequence, by finding of identical elements of a key, allows to reveal possible areas of modification of the image.*

*Ключевые слова: защита информации, стеганография, цифровой водяной знак, модуляция яркости.*
*Key words: information security, steganography, digital watermark, intensity modulation.*

## Введение

Огромное количество электронных документов, циркулирующих в компьютерных сетях, является основанием для постановки важной задачи защиты информации, хранящейся в данных документах. Необходимо обеспечить защиту документов от несанкционированного доступа или от преднамеренных искажений сообщений [1]. Задача надежной защиты авторских прав, прав интеллектуальной собственности и других конфиденциальных данных от несанкционированного доступа является одной из важнейших и не до конца решенных до настоящего времени проблем.

В соответствии со ст. 23 Конституции РФ, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Совокупность правовых норм, закрепленных в главе 14 Трудового кодекса РФ, впервые регулирует отношения по сбору, обработке, хранению, использованию и передаче персональных данных работника. Информация, относящаяся к коммерческой тайне, имеет особую материальную ценность для организаций. Отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации и охраной ее конфиденциальности регулирует вступившая в силу с 01 января 2008 г. ч. IV ГК РФ и ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Водный транспорт, напрямую зависящий от наличия безопасных средств управления, систем навигации и связи, обязан оказывать повышенное внимание в отрасли технологическому обновлению, внедрению высокопроизводительных систем автоматизации, применению инновационных технологий [2]. Для хранения и передачи такого огромного количества информации нужны соответствующие системы автоматизации, позволяющие обезопасить всю процедуру обработки документов различного рода. Тем самым развитие информационных технологий в транспортных компаниях и, в частности, на судах напрямую связано с построением систем обработки информации [3], [4].

Предметом данной статьи является разработка и исследование алгоритма внедрения цифрового водяного знака (ЦВЗ) на основе модуляции яркости блоков графических документов, позволяющего одновременно обеспечивать скрытое встраивание произвольной информационной последовательности заданного объёма и аутентификацию изображения, в которое был встроен ЦВЗ.

## Основная часть

В качестве контейнеров передачи скрытой информации могут выступать различные оцифрованные данные: растровые графические изображения, звук, видео, всевозможные носители цифровой информации, а также текстовые и другие электронные документы. Наиболее распространенными типами контейнеров в компьютерной стеганографии на данный момент являются изображения и аудиоданные, представленные в цифровой форме, а также видеопоследовательности, т. е. мультимедиаконтейнеры [5]. Это объясняется тем, что подобные контейнеры уже по технологии получения имеют шумовую составляющую, которая маскирует встраиваемое сообщение.

Довольно большой процент современных систем компьютерной стеганографии использует в качестве контейнеров растровые графические изображения различных форматов. Наиболее широкое распространение в последнее время получил формат JPEG [6], [7], в котором практически все современные цифровые фотоаппараты и видеокамеры сохраняют изображения (большинство фотографических изображений опубликованы в сети интернет именно в нем). В том случае, когда формат хранения растровых изображений использует сжатие данных, значительно возрастает сложность разработки стеганографической системы, так как, во-первых, увеличивается сложность анализа формата, а во-вторых, изменения, вносимые стеганографической системой в данные изображения, приводят к нежелательному ухудшению эффективности сжатия [8]. В случае, когда формат графических изображений использует сжатие с потерями информации, классические ме-

тоды сокрытия в графических изображениях, как правило, становятся малоэффективными, так как при потере информации происходит уничтожение скрытой информации, в силу малой амплитуды сокрытого сигнала. Для повышения робастности вложения встроенных ЦВЗ к сжатию графических документов в стегоалгоритмах необходимо применять те же преобразования, что и в алгоритмах сжатия этих файлов.

Важнейшей особенностью формата JPEG является использование алгоритма сжатия информации с потерями. Это означает, что при сжатии файла часть информации уничтожается, но изменения незначительно влияют на файл, и они малозаметны. Формат JPEG предназначен, в первую очередь, для изображений с плавными цветовыми переходами и градиентами, таких как обычные цифровые фотографии. Благодаря этому фактору именно данный тип графических документов имеет такой успех среди большого количества передаваемой информации.

Необходимо проверить, насколько зависимы два соседних пикселя. Проверим это для всех пар пикселей изображения. Отметим их на координатной плоскости точками так, что координата точки по оси абсцисс — значение первого пикселя, по оси ординат — второго. Для изображения размером 256 × 256 получим 32768 точек (рис. 1).

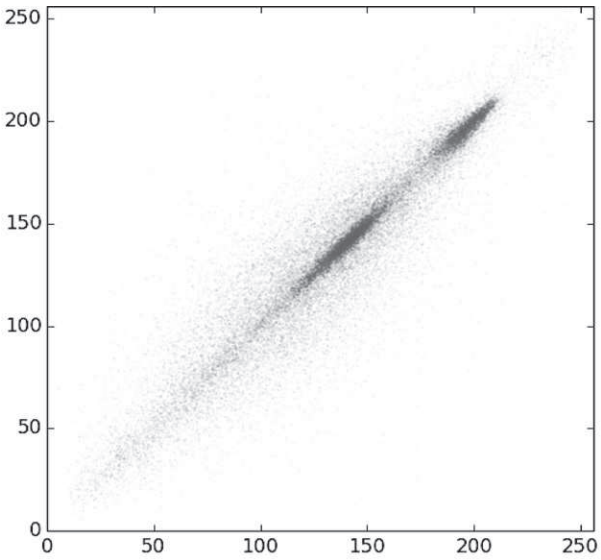


*Рис. 1.* Зависимость пар соседних пикселей

Каков бы ни был алгоритм сжатия информации, его принцип всегда один — нахождение и описание закономерностей. Чем больше закономерностей, тем больше избыточности, тем меньше информации [9]. Архиваторы и кодеры обычно приспособлены под конкретный тип информации, и знают, где можно их найти. В некоторых случаях закономерность видна сразу, например, картина голубого неба. Каждый ряд его цифрового представления можно довольно точно описать прямой [10].

На первом этапе при сжатии изображения форматом JPEG происходит преобразование из цветового пространства *RGB*, широко используемого в компьютерной графике, в пространство $YC_bC_r$, основанное на характеристиках яркости и цветности. Применение данного пространства вместо привычного и легкого для понимания *RGB* объясняется физиологическим строением человеческого глаза, а именно нервной системой человеческого зрения, которая обладает гораздо большей чувствительностью к яркости нежели к цветоразностным составляющим. Буква *Y* в таких цветовых пространствах обозначает компонент *светимость*, которая вычисляется как взвешенное усреднение компонентов *R*, *G* и *B* по следующей формуле:

$$Y = k_r R + k_g G + k_b B,$$

где *k* — соответствующий весовой множитель.

Остальные цветовые компоненты, по существу, определяются в виде разностей между светимостью $Y$ и компонентами $R$, $G$ и $B$:

$$C_b = B - Y;$$
$$C_r = R - Y;$$
$$C_g = G - Y;$$

При этом получаются четыре компонента нового пространства вместо трех *RGB*. Однако число $C_b + C_r + C_g$ является постоянным, поэтому только два из трех хроматических компонентов необходимо хранить, а третий можно вычислять на основе двух других. Чаще всего в качестве двух искомых цветовых компонентов используют $C_b$ и $C_r$. Преимущество пространства $YC_bC_r$ по сравнению с *RGB* заключается в том, что $C_b$ и $C_r$ можно представлять с меньшим разрешением, чем $Y$, так как глаз человека менее чувствителен к цвету предметов, чем к их яркости. Это позволяет сократить объем информации, необходимой для представления хроматических компонентов, без заметного ухудшения качества передачи цветовых оттенков изображения. Такой подход к преобразованию цветового пространства дает дополнительный эффект при сжатии цветных изображений. При этом алгоритмы сжатия сначала преобразуют исходное цветовое пространство из *RGB* в $YC_bC_r$, сжимают его, а затем при восстановлении обратно преобразуют изображение в цветовое пространство *RGB*, так как оно используется в ЭВМ. Формулы для прямого и обратного преобразований выглядят следующим образом:

$$\left.\begin{aligned} Y &= k_r R + (1-k_b-k_r)G + k_b B; \\ C_b &= \frac{0,5}{1-k_b}(B-Y); \\ C_r &= \frac{0,5}{1-k_r}(R-Y). \end{aligned}\right\} \quad (1)$$

$$\left.\begin{aligned} R &= Y + \frac{1-k_r}{0,5}C_r; \\ G &= Y - \frac{2k_b(1-k_b)}{1-k_b-k_r}C_b - \frac{2k_r(1-k_r)}{1-k_b-k_r}C_r; \\ B &= Y + \frac{1-k_b}{0,5}C_b. \end{aligned}\right\} \quad (2)$$

На втором этапе яркостный компонент $Y$ и отвечающие за цвет компоненты $C_b$ и $C_r$ разбиваются на блоки 8 × 8 пикселей и отдельно для каждого компонента цветового пространства $YC_bC_r$ осуществляется прямое дискретно-косинусное преобразование:

$$DCT(i,j) = \frac{1}{\sqrt{2N}}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}p(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2x+1)j\pi}{2N}\right];$$

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}}, & x = 0; \\ 1, & x > 0. \end{cases}$$

Цель этого преобразования заключается в переходе от пространственного представления изображения к спектральному (пространству частот изменения яркости и оттенка). Именно на данном этапе большинство алгоритмов внедряет ЦВЗ в графический документ. Если не переходить к данному этапу, а воспользоваться зависимостью значений яркости близлежащих блоков пикселей, то можно сделать вывод, что поскольку яркостный компонент подвергается меньшим изменениям, то можно производить встраивание информации именно в данный параметр.

Предлагаемый метод основан на широко известном методе QIM (*Quantization Index Modulation*) с использованием модуляции яркости пикселей изображения [11]. Пусть даны исход-

ное изображение $I(n, m)$ и бинарное изображение ЦВЗ $W(n, m)$, где $n \in [1, N]$; $m \in [1, M]$. Предлагаемый в данной работе алгоритм предполагает встраивание ЦВЗ по следующему правилу:

При $W(n, m) = 1$:
если $I(n, m) > I(n, m+1)$, тогда $I'(n, m) = I(n, m)$,
иначе $I'(n, m) = I(n, m) + P$.

При $W(n, m) = 0$:
если $I(n, m) < I(n, m+1)$, тогда $I'(n, m) = I(n, m)$,
иначе $I'(n, m) = I(n, m) - P$.

Здесь $P$ — минимальный уровень аддитивного сигнала, позволяющий изменить яркость пиксела настолько, чтобы алгоритм сжатия не только смог его пережать, но и внешне был незаметен человеческому глазу.

Так как алгоритм сжатия JPEG работает поблочно, перераспределение яркости необходимо производить на участках блоков размером 8 × 8 пикселей, иначе вся модуляция яркости, выполненная на данном этапе, при квантовании JPEG будет нарушена.

Третий этап алгоритма является основным. Именно здесь происходит внедрение ЦВЗ в контейнер изображения при помощи перераспределения яркости внутри блоков по всему полотну изображения. Работает это следующим образом. Все цифровое изображение ЦВЗ является черно-белым (бинарным), соответственно можно провести аналогию и задать для белого цвета бит, равный «0», а для черного — «1». Предположим, что существует необходимость внедрить в графический цифровой файл бит, равный «0». Для этого необходимо вначале в изображении-исходнике выполнить расчет разности показателей яркости блоков пикселей. Для удобства рассмотрим случай без использования хэш-функций псевдослучайного распределения блоков и будем строить последовательности блоков по их следованию в изображении. Для вычисления значения яркости будем использовать следующую формулу:

$$Y = 0{,}3R + 0{,}59G + 0{,}11B,$$

где $R$, $G$, $B$ — значения красного, зеленого и синего цветов соответственно.

Возьмем два соседних блока 8 × 8 пикселей оцифрованного изображения и рассчитаем средний показатель яркости для каждого из них.

а) б)

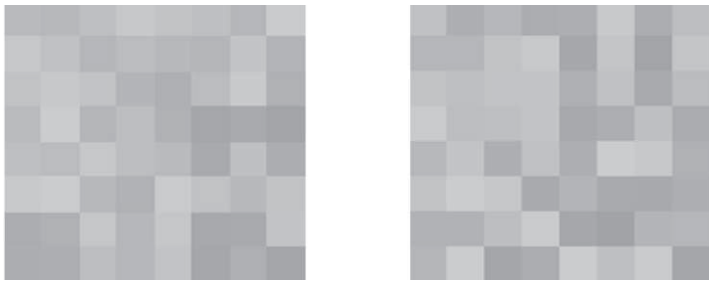

*Рис. 2.* Средние показатели яркости двух сосдених блоков:
*а* — $Y = 162.978$; *б* — $Y = 161.468$

Для внедрения бита со значением «0» необходимо, чтобы первый блок имел усредненное значение яркости меньше, чем второй. Здесь необходимо произвести перераспределение яркости.

Для модуляции яркости воспользуемся равномерным законом распределения вероятностей:

$$f(x) = \begin{cases} \dfrac{1}{b-a}, & a \le x \le b; \\ 0, & x < a, x > b. \end{cases}$$

Последним этапом сокрытия ЦВЗ является псевдослучайное распределение разностных блоков 8 × 8, т.е. не прямолинейное движение слева-направо между соседними блоками, а вычисление разности между блоками, находящимися в случайных позициях изображения. Этого можно добиться, используя специальный ключ — хеш-функцию, генерируемую на основе пароля, вводимого отправителем. Таким образом, алгоритм кодирования приобретает следующий вид:

1 — генерирование хэш-функции на основе пароля;

2 — разбиение входного изображения на блоки размером 8 × 8 пикселей;

3 — вычисление разницы между блоками, определенными хеш-функцией;

4 — перераспределение яркости внутри блока.

Для декодирования используются те же самые операции, выполненные в обратную сторону, с некоторыми дополнениями:

1 — генерирование хэш-функции на основе пароля;

2 — разбиение входного изображения на блоки размером 8 × 8 пикселей;

3 — вычисление разницы между блоками, определенными хеш-функцией;

4 — построение фрагментов ЦВЗ;

5 — извлечение и восстановление ЦВЗ путем сложения всех фрагментов.

Если изображение потеряло часть информации или в него были внесены модификации, то ЦВЗ при извлечении подвергается процедуре восстановления, исследуя поблочно всё изображение и находя одинаковые элементы ключа [12]. Таким образом, модификация одного или нескольких блоков изображения-контейнера приводит к потере только соответствующих бит (пикселей), не оказывая влияния на извлечение других бит для восстановления ЦВЗ. Это означает, что ЦВЗ не только будет восстановлен, но и будут обнаружены места нарушения внедрения ЦВЗ, а следовательно, модификации изображения [13].

В качестве иллюстрации предложенного алгоритма и его свойств встроим в изображение-контейнер ЦВЗ размером 25 × 10 пикселей, после чего подвергнем изображение с внедренным ЦВЗ ряду геометрических атак и сжатию форматом JPEG (рис. 3). Из-за кадрирования произошло смещение границ блоков встраивания, вследствие чего произошел сдвиг ЦВЗ. Также цифровой знак потерял 10 % информации, при том, что оригинал изображения-контейнера потерял порядка 40 %. При таких колоссальных модификациях изображения цифровой знак остался хорошо читаемым, а также показал возможные варианты модифицированных областей. Данные результаты показывают, что ЦВЗ, встроенный с использованием разработанного алгоритма, обладает устойчивостью к набору геометрических преобразований изображения-контейнера, а также сжатию форматом JPEG.

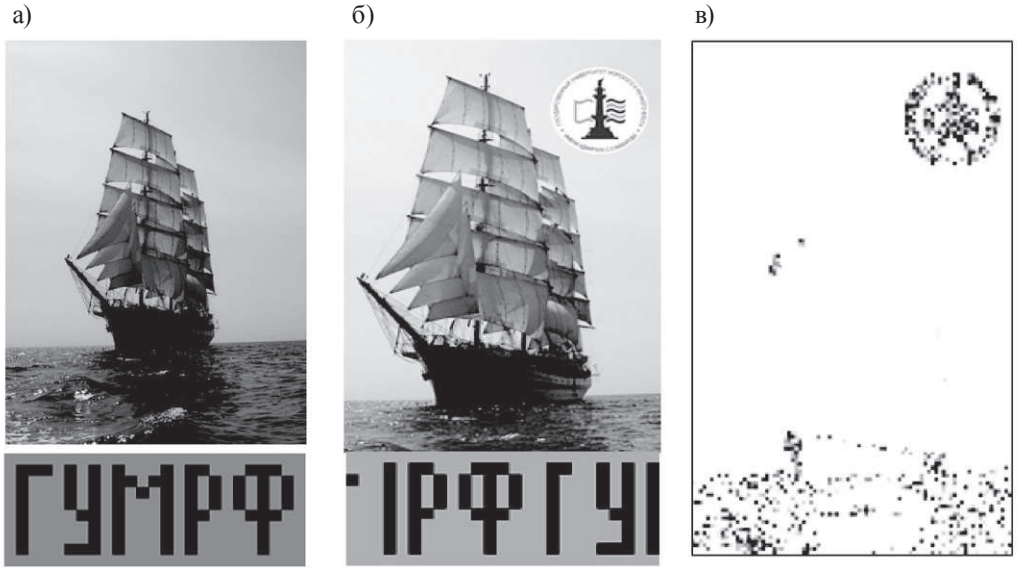


*Рис. 3.* Результат извлечения ЦВЗ из модифицированного изображения:
*а* — изображение-контейнер и встраиваемый ЦВЗ;
*б* — модифицированное изображение и извлеченный ЦВЗ;
*в* — области модификации изображения-контейнера

**Заключение**

В настоящей работе представлен новый алгоритм поблочного встраивания ЦВЗ, обладающий следующими преимуществами по сравнению с существующими методами.

1. Алгоритм позволяет одновременно встраивать произвольный ЦВЗ в изображение-контейнер и обеспечивать проверку поблочной подлинности изображения.

2. Алгоритм обеспечивает устойчивость ЦВЗ к преобразованиям кадрирования, линейного контрастирования, замене произвольных фрагментов изображения.

3. Алгоритм не требует использования дополнительных процедур предобработки (в частности, шифрования) изображения ЦВЗ.

4. Алгоритм не требует использования фиксированного ЦВЗ для обнаружения модификаций, что обеспечивает стойкость ЦВЗ к так называемым «атакам с фиксированным ЦВЗ» (watermarktemplateattack, преднамеренная атака осведомлённого нарушителя, позволяющая скрывать модификации изображения даже при наличии встроенного ЦВЗ).

5. Алгоритм работает быстрее за счет использования модуляции яркости, а не расчета матриц дискретно косинусного преобразования.

Использование перераспределения яркости в качестве основы сокрытия информации дает неограниченные возможности по улучшению алгоритма. Возможно использование различных алгоритмов распределения яркости внутри блоков для более плотного внедрения битов ЦВЗ, коррекция границ участков блоков с ярко выраженным перераспределением яркости. Также можно добавить процедуру восстановления ЦВЗ для изображений, повернутых на угол, кратный 90 °.

**Список литературы**

1. *Сабанов А.* Некоторые аспекты защиты электронного документооборота / А. Сабанов // Connect. Мир связи. — 2010. — № 7. — С. 62–64.

2. *Каторин Ю. Ф.* Защищенность информации в каналах передачи данных в береговых сетях автоматизированной идентификационной системы / Ю. Ф. Каторин, В. В. Коротков, А. П. Нырков // Журнал университета водных коммуникаций. — 2012. — № 1. — С. 98–102.

3. *Лубенец А.* Пути повышения эффективности документооборота на транспорте / А. Лубенец // Автоматизация транспортной отрасли. — 2010. — № 4. — С. 18–19.

4. *Нырков А. П.* Безопасность данных протокола SOAP в системах управления движением судов / А. П. Нырков, Д. С. Власов // X Санкт-Петербургская международная конференция «Региональная информатика — 2006» (РИ-2006): тр. конф. — СПб.: СПОИСУ, 2007. — С. 210–213.

5. *Шмаев В. Б.* Современная стеганография. Принципы, основные носители и методы противодействия / В. Б. Шмаев // Эссе по курсу «Защита информации». — 2010. — С. 1–3.

6. *Шилихина В. А.* Модель обеспечения целостности при преобразованиях стеганоконтейнера с потерями / В. А. Шилихина, А. В. Никишова // Материалы второй всероссийской науч.-практ. конф. — Волгоград, 2013. — С. 50–51.

7. *Конахович Г. Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — М.: МК-Пресс, 2006. — 288 с.

8. *Миано Дж.* Форматы и алгоритмы сжатия изображений в действии / Дж. Миано. — М.: ТРИУМФ, 2005. — 330 с.

9. *Кустов В. Н.* Методы встраивания скрытых сообщений / В. Н. Кустов, А. А. Федчук // Защита информации. Конфидент. — 2010. — № 3. — С. 34–41.

10. *Барсуков В. С.* Стеганографические технологии защиты документов, авторских прав и информации / В. С. Барсуков // Обзор специальной техники. — 2009. — № 2. — С. 31–40.

11. *Глумов Н. И.* Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н. И. Глумов, В. А. Митекин // Компьютерная оптика. — 2011. — Т. 35. — № 2. — С. 262–264.

12. *Бухарметов М. Р.* Использование нейронных сетей для безопасного электронного документооборота на транспорте / М. Р. Бухарметов // Сб. работ междунар. науч.-практ. конф. «Информационные управляющие системы и технологии». — Одесса, 2014. — С. 167–169.

13. *Бухарметов М. Р.* Методы обеспечения защищенного документооборота в транспортной сфере / М. Р. Бухарметов // Сб. «Информационная безопасность регионов России (ИБРР-2013)». — СПб., 2013. — С. 87–88.

**УДК 004.042, 004.942, 681.3.07**

**Б. Н. Попов**,
канд. техн. наук, доц.;

**Е. С. Федорина**,
асп.

# ПРИМЕНЕНИЕ МЕТОДОВ АНАЛИЗА И ОБРАБОТКИ ДАННЫХ К ИНФОРМАЦИОННЫМ ПОТОКАМ ОБЪЕКТОВ ВОДНОГО ТРАНСПОРТА

# USING OF METHODS FOR ANALYSIS AND PROCESSING DATA TO AN INFORMATION FLOWS FOR OBJECTS OF WATER TRANSPORT

*Статья посвящена вопросам анализа и обработки потоков данных в информационных системах объектов водного транспорта. Рассмотрено понятие информационного потока для сложных данных воднотранспортной отрасли. В качестве методов анализа и обработки информационного потока выбраны нелинейное вейвлет-преобразование (НВП) и дискретное преобразование Фурье (ДПФ). Приведены формулы для НВП и ДПФ, описана главная идея НВП для сигналов, представляющих информационный поток. Смоделированы различные виды сигналов, представляющие необработанные информационные потоки. Для этих сигналов проведено НВП в пакете Wavelet Toolbox системы MATLAB. Результаты НВП приведены в графическом виде. Применено ДПФ к зашумленному сигналу, представлен график спектральной плотности этого сигнала. Приведены выводы по проделанной работе.*

*The article is developed to questions of analysis and processing of data flows in information systems for objects water transport. The concept of information flow is considered for complex data of a water-transport branch. Continuous Wavelet conversion and discrete Fourier conversion are chosen as methods of analysis and processing of information flows. Continuous Wavelet conversion and discrete Fourier conversion are given and the main idea of Wavelet conversion is described for signals representing information flows. Different view of signals representing untreated information flows. Continuous Wavelet conversion is conducted for these signals in Wavelet Toolbox package of MATLAB system. Results of Wavelet conversion are given in the graphic view. Discrete Fourier conversion is applied to the noisy signal; the graph of the spectral density is represented of the signal. The conclusions are given by made the work.*

*Ключевые слова: информационный поток, непрерывное вейвлет-преобразование, дискретное преобразование Фурье, скейлограмма, пакет Wavelet Toolbox системы MATLAB.*

*Key words: information flow, continuous Wavelet conversion, discrete Fourier conversion, skeylogramma, Wavelet Toolbox package of MATLAB system*



В СОВРЕМЕННОМ мире информационные системы (ИС) находят применение в самых различных сферах деятельности общества, в том числе — на объектах водного транспорта (ОВТ) [1], [2]. Для ОВТ характерны распределенные ИС [3], их компоненты представ-