Государственное научное учреждение
«Объединенный институт проблем информатики
Национальной академии наук Беларуси»

УДК 003.26+347.78

ШУТЬКО Надежда Павловна

ЗАЩИТА ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ НА ТЕКСТОВЫЕ ДОКУМЕНТЫ МЕТОДАМИ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Автореферат диссертации
на соискание ученой степени кандидата технических наук
по специальности 05.25.05 — «Информационные системы и процессы»

Минск 2016

Работа выполнена в учреждении образования «Белорусский государственный технологический университет»

Научные руководители:	**ЛИСТОПАД Николай Измайлович,** доктор технических наук, профессор, заведующий кафедрой информационных радиотехнологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»; **РОМАНЕНКО Дмитрий Михайлович,** кандидат технических наук, доцент, заведующий кафедрой информатики и веб-дизайна учреждения образования «Белорусский государственный технологический университет»
Официальные оппоненты:	**ГОЛИКОВ Владимир Федорович,** доктор технических наук, профессор, заведующий кафедрой информационных технологий в управлении Белорусского национального технического университета **БЕЛОДЕД Николай Иванович,** кандидат технических наук, доцент, профессор кафедры управления информационными ресурсами Академии управления при Президенте Республики Беларусь
Оппонирующая организация	Белорусский государственный университет

Защита состоится 29 ноября 2016 г. в 14.30 на заседании совета по защите диссертаций Д 01.04.01 при государственном научном учреждении «Объединенный институт проблем информатики Национальной академии наук Беларуси» по адресу: 220012, г. Минск, ул. Сурганова, 6, зал заседаний. Телефон ученого секретаря: (+375 17) 284 21 68, факс (+375 29) 284 21 75, e-mail: lipn@newman.bas-net.by.

С диссертацией можно ознакомиться в библиотеке Объединенного института проблем информатики НАН Беларуси.

Автореферат разослан «24» октября 2016 г.

Ученый секретарь совета
по защите диссертаций
доктор технических наук, доцент С. Ф. Липницкий

КРАТКОЕ ВВЕДЕНИЕ

Информационные системы и процессы стали определяющим фактором реализации инновационного подхода, повышения эффективности решений, принимаемых в научной, экономической, управленческой и других видах целенаправленной деятельности.

Развитие ИТ-сферы неразрывно связано, в том числе, с переходом на электронный документооборот, в частности, и с разработкой технологий и инструментальных средств создания, хранения и использования цифрового контента вообще. Важную часть этого контента составляет, например, сегмент электронных образовательных ресурсов, а также репозитории учрежденческих, ведомственных или иных документов, которые представляют коммерческую ценность или относятся к объектам авторского права.

В силу перечисленных особенностей особой актуальностью характеризуется проблема защиты электронных документов от несанкционированного использования или модификации, а также защиты и доказательства прав интеллектуальной собственности. В настоящее время бремя защиты авторских прав лежит на самом авторе или на правообладателе авторских прав. Из этого следует, что автор или правообладатель, прежде чем помещать документ в Интернете, должны предварительно позаботиться о реализации мер по защите своих авторских прав.

Настоящее диссертационное исследование выполняется в рамках указанной проблемы и направлено на решение задачи по защите права интеллектуальной собственности на электронные текстовые документы.

Основой для разработки достаточно универсальных инструментальных средств защиты контента в течение последних примерно 15 лет стали методы и алгоритмы текстовой стеганографии, которые базируются на общих теоретических положениях и результатах прикладных исследований стеганографического преобразования информации, сформулированных в работах Дж. Фридриха (J.Fridrich), С. Воложинского (S. Voloshynovskiy), В. Бендера (W. Bender), Н. Моримото (N. Morimoto), Р. Поупа (R. Popa), Б. Пфицмана (B. Pfitzmann), М. Куттера (M. Kutter), а также В. Г. Грибунина, Г. Ф. Конаховича, Ю. С. Харина, В. Н. Ярмолика и др. Базовые идеи для разработки методов текстовой стеганографии, которые могут быть адаптированы к задачам защиты прав интеллектуальной собственности, описаны в ряде работ Дж. Брассила (J.Brassil) и Н. Максэмчука (N.Maxemchuk). В известных публикациях исследуются

методы осаждения тайной (авторской) информации в текстовый документ путем модификации межсловарного пробела или межстрочного расстояния (интерлиньяжа). Использование других элементов шрифтового оформления текстового документа открывает дополнительные возможности по повышению эффективности защиты авторских прав на такие документы. Этот тезис является дополнительным подтверждением актуальности диссертационного исследования.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами, темами. Тема диссертационного исследования соответствует приоритетным направлениям научно-технической деятельности в Республике Беларусь на 2011-2015 гг. (Указ Президента Республики Беларусь от 22 июля 2010 г. № 378 «Об утверждении приоритетных направлений научно-технической деятельности в Республике Беларусь на 2011-2015 годы») и на 2016-2022 гг. (Указ Президента Республики Беларусь от 22 апреля 2015 г. № 166 «О приоритетных направлениях научно-технической деятельности в Республике Беларусь на 2016-2020 годы»). Исследования проводились на кафедре информационных систем и технологий УО БГТУ в рамках научно-исследовательских госбюджетных тем: НИР ГБ 11-165 «Методы и программные средства хеширования сообщений и обмена конфиденциальной информацией на основе нейросетевых технологий» (ГР № 20111584, ГПИНИ «Информатика и космос», задание 1.5.11); НИР ГБ 11-025 «Разработка и анализ стеганографических методов для защиты прав интеллектуальной собственности на текстовые документы» (ГР №20111345, грант Министерства образования Республики Беларусь); НИР ГБ 14-167 «Разработка методов и программных средств защиты авторских прав на электронные текстовые документы и программные коды на основе стеганографии и обфускации» (ГР № 20141362, задание 1.33 ГПНИ «Информатика и космос»); НИР ГБ 16-113 «Методы и алгоритмы стеганографической защиты данных в компьютерных сетях с учетом свойств форматов данных и их конвертации» (ГР № 20161347, ГПНИ «Информатика, космос и безопасность», задание 1.2.01 подпрограммы «Информатика и космические исследования»).

Цель и задачи исследования. *Цель*: разработка и анализ эффективных методов и инструментальных средств текстовой стеганографии, основанных на модификации цветовых и пространственно-

геометрических параметров символов текста, для решения задач по обеспечению авторского права на электронные текстовые документы.

Для достижения поставленной цели требуется решить следующие *задачи*:

1) проанализировать текущее состояние проблемы охраны авторских прав на электронные текстовые документы, а также особенности использования методов текстовой стеганографии с целью обеспечения эффективного хранения и передачи тайной информации в компьютерных стеганографических системах;

2) разработать математическую модель стеганографической системы, основанной на использовании ключевой информации, обеспечивающей повышенный уровень стеганографической стойкости системы;

3) разработать новые эффективные синтаксические методы стеганографии на основе модификации цветовых и пространственно-геометрических параметров символов текста защищаемого документа;

4) разработать алгоритмы осаждения и извлечения информации на основе предложенных стеганографических методов;

5) разработать программные средства для реализации, анализа параметров и эффективности использования разработанных стеганографических методов.

Научная новизна полученных результатов:

1) в основу разработанных стеганографических методов, реализующих их алгоритмов и необходимого математического обеспечения положена идея использования цветовых и пространственно-геометрических параметров символов защищаемого текста (апрош, кернинг), модификация которых позволяет осаждать/извлекать тайную информацию;

2) обоснован и исследован новый подкласс стеганографических систем, определенный как «многоключевые стеганографические системы»; в основе разработанной математической модели таких систем используется теоретико-множественное определение, взаимосвязь и взаимозависимость основных компонент системы, представляющей собой совокупность множеств сообщений M, контейнеров C, основных ключей K^{o}, дополнительных ключей первого рода $K^{д1}$, дополнительных ключей второго рода $K^{д2}$, стегоконтейнеров (заполненных контейнеров) S и преобразований (прямого F — осаждение сообщения, и обратного F^{1} — извлечение сообщения), которые их связывают;

3) методика оценки эффективности разработанных и известных методов текстовой стеганографии основана на использовании и анализе введенного показателя «плотности заполнения стегоконтейнера»: заполнение «пустого» контейнера C_j ($C_j \in \mathbb{C}$), который представляет собой защищаемый документ, символами (знаками) тайного сообщения M_i ($M_i \in \mathbb{M}$); этот показатель количественно определяется отношением числа стегознаков (символов текста-контейнера, в которые производится осаждение информации) к общему числу знаков в таком контейнере.

Положения диссертации, выносимые на защиту.

1. Математическая модель многоключевой стеганографической системы, основанная на теоретико-множественном определении основных компонент системы, представляющей собой совокупность множеств сообщений, контейнеров, основных ключей, дополнительных ключей первого рода, дополнительных ключей второго рода, стегоконтейнеров (заполненных контейнеров) и преобразований, которые их связывают, характеризующаяся в сравнении с известными моделями более высокой степенью адекватности, достигаемой увеличением числа существенных параметров модели в виде дополнительных ключей. Это позволило синтезировать структурную схему стеганографической системы на более высоком уровне детализации.

2. Синтаксические методы текстовой стеганографии, основанные на модификации цветовых и пространственно-геометрических (апрош, кернинг) параметров символов текста и обеспечивающие увеличение до 90 % объема осаждаемой информации и повышение в 2–4 раза стойкости стегоконтейнера к взлому на основе визуального анализа в сравнении с известными методами.

3. Алгоритмы прямого (осаждение тайной информации в электронный текстовый документ-контейнер) и обратного (извлечение осажденной информации) стеганографических преобразований, реализующие разработанные синтаксические методы, что позволило создать и зарегистрировать в национальном центре интеллектуальной собственности Республики Беларусь 3 импортозамещающих программных средства.

4. Методика оценки эффективности разработанных и известных методов текстовой стеганографии, основанная на использовании и анализе введенного показателя «плотности заполнения стегоконтейнера», и методика оценки стойкости стегоконтейнера к взлому на основе визу-

ального анализа цветовых и пространственно-геометрических параметров символов текста-контейнера, позволяющие сформировать показатели качества методов текстовой стеганографии.

Личный вклад соискателя. Все результаты, приведенные в диссертации, получены либо соискателем, либо при его непосредственном участии. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертации результатов. Участие автора в создании программных средств касалось постановки задачи, разработки схемы функционирования приложений, структуры его интерфейса и диалоговых окон. Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научными руководителями.

Апробация результатов диссертации и информация об использовании ее результатов. Основные положения и результаты диссертационной работы были представлены на следующих научно-технических конференциях: Республиканская научная конференция студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и в научных исследованиях» (Гомель, 2009, 2011, 2013); Международная научно-техническая конференция студентов и аспирантов «Друкарство молоде» (Киев, Украина; 2010, 2011); Международная конференция молодых ученых «Print–2011» (Санкт-Петербург, Россия; 2011); International Conference «New electrical and electronic technologies and their industrial implementation» (Закопане, Польша; 2011, 2013, 2015); International Scientific Conference on Printing and Media Technology «Printing future days» (Хемниц, Германия; 2011, 2015); Международная научно-техническая конференция «Автоматический контроль и автоматизация производственных процессов» (Минск, БГТУ, 2012); Международная научная конференция «Информационные технологии и системы» (Минск, БГУИР, 2012); Всероссийская научно-техническая конференция студентов и аспирантов «Микроэлектроника и информатика–2014» (Зеленоград, Россия; 2014); Международная научно-техническая конференция «ITI-2015» (Минск, ОИПИ, 2015) и др.

На основе предложенных в работе решений созданы и зарегистрированы в Национальном центре интеллектуальной собственности Республики Беларусь 3 компьютерные программы, являющиеся импортозамещающими средствами. Результаты диссертационной работы внедрены и используются в унитарном предприятии «Инфотех» (Минск) при разра-

ботке программного модуля «Криптошифр», а также в учебном процессе УО «Белорусский государственный технологический университет».

Опубликованность результатов. По результатам выполненных исследований опубликовано 39 печатных работ (4,35 а. л.), в том числе: 8 статей в рецензируемых научных журналах и материалах зарубежных НТК (4 из них — в научных изданиях, входящих в Перечень ВАК Республики Беларусь, 4 — в зарубежном научном журнале, включенном в базу данных Scopus), тезисы 28 докладов и материалов конференций, 3 свидетельства о регистрации компьютерных программ. Без соавторов опубликовано 12 работ.

Структура и объем диссертации. Работа состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, включающего 122 наименования, списка публикаций соискателя, приложения. Общий объем — 124 страницы, в том числе 55 иллюстраций, 9 таблиц.

ОСНОВНАЯ ЧАСТЬ

Во **введении** обоснована актуальность исследования, дана общая характеристика предметной области и определено направление диссертационной работы.

В **первой главе** выполнен анализ современного состояния проблемы защиты авторского права в ИТ-отрасли, в частности, защиты электронных текстовых документов от незаконного использования, а также анализ направлений по решению основных задач в данной предметной области. Проведенный анализ выявил следующее:

1) в настоящее время в Республике Беларусь созданы важные компоненты нормативно-правовой базы, обеспечивающей охрану авторских прав, в том числе — в ИТ-области;

2) существует многообразие инструментальных средств, предназначенных, в основном, для защиты мультимедийных или графических файлов-документов. Имеющиеся на рынке средства для защиты текстовых документов созданы коммерческими организациями для собственного применения при продаже или распространении продукции на платной основе;

3) важнейшей особенностью стеганографической информационной системы охраны права собственности является то, что она

выполняет функции, схожие с функциями электронной цифровой подписи: осаждаемая (тайная) информация используется не только как инструмент защиты авторства, но и, в определенной степени, влияет на целостность охраняемого объекта, а также сама зависит от этой целостности.

На рисунке 1 приведена обобщенная схема стеганографической системы. Эта структура и ее компоненты взяты нами за основу для решения поставленных задач.

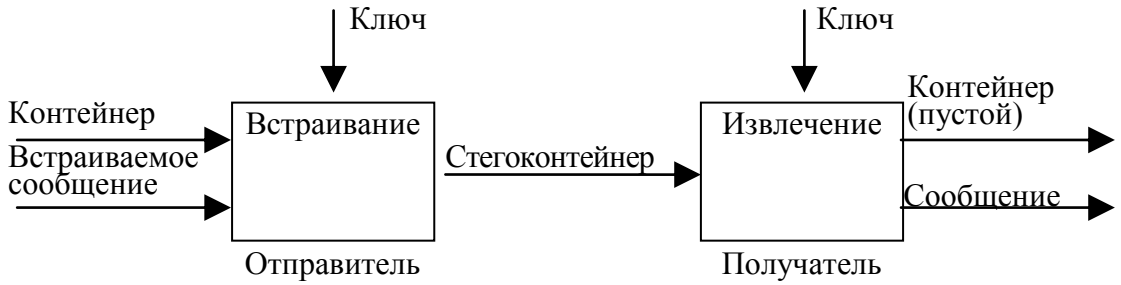

Рисунок 1. — Общая схема стеганографической системы

Применительно к задачам исследования *контейнер* (*файл-контейнер* или *документ-контейнер*) — любой текстовый документ, предназначенный для *сокрытия* (*осаждения*, *embedding*) в нем тайного (авторского) сообщения; *ключ* (*стеганоключ* или *стегоключ*, *stego-key*) — секретный ключ, являющийся аналогом криптографического ключа и необходимый для осаждения и извлечения секретной информации. Стеганографическое преобразование наиболее часто осуществляется с использованием одного ключа, который определяет алгоритм осаждения/извлечения. Осаждаемая (встраиваемая или авторская) путем модификации контейнера информация и будет являться, в случае необходимости, при ее *извлечении* доказательством авторства и поможет, таким образом, защитить интеллектуальную собственность. Свойства контейнера должны быть модифицированы так, чтобы это невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия сообщения.

В диссертации подробно проанализированы достоинства и недостатки существующих стеганографических методов (в том числе — метода наименее значащего бита, LSB, методов Word-Shift Coding и Line-Shift Coding.

Формальное описание стеганографической системы основывается на взаимосвязи элементов соответствующих множеств: *сообщения M* ($M \in \boldsymbol{M}$, $\boldsymbol{M}$ — множество всех сообщений); *контейнера C* ($C \in \boldsymbol{C}$, $\boldsymbol{C}$ —

множество всех контейнеров); *ключа* K ($K \in \boldsymbol{K}$, $\boldsymbol{K}$ — множество всех ключей); *заполненного контейнера* (*стегосообщения*) S ($S \in \boldsymbol{S}$, $\boldsymbol{S}$ — множество всех стегосообщений).

Стеганографический алгоритм составляют два преобразования, задаваемые на основе отображений: прямое преобразование F, сопоставляющее сообщению, пустому контейнеру, ключу заполненный контейнер, и обратное F^{-1}:

$$F: M \times C \times K \rightarrow S;\ F^{-1}: S \times K \rightarrow M. \qquad (1)$$

Принципиальным, с нашей точки зрения, для описания системы, характеристики и оценки ее стойкости к любым изменениям или несанкционированным действиям является определение и детализация ключевой информации.

Во **второй главе** приведено описание разработанной математической модели универсальной стеганографической системы, основанной на использовании нескольких типов ключевой информации. В основу разработанных методов и соответствующей им модели положены важнейшие пространственно-геометрические и цветовые характеристики базовых элементов текстовых шрифтов, а также соотношение (1).

Принято, что множество $\boldsymbol{M}$ сообщений M_i является конечным: $\boldsymbol{M} = \{M_1, M_2, \ldots, M_n\}$; $\boldsymbol{C}$ — это конечное множество всех допустимых контейнеров C_j (файлов-контейнеров или документов-контейнеров) — объектов защиты: $\boldsymbol{C} = \{C_1, C_2, \ldots, C_p\}$, причем $p > n$; $\boldsymbol{K}$ — множество всех ключей, под которыми в общем случае понимаются методы или алгоритмы осаждения сообщения в контейнер (отождествляются с основным ключом, входящим во множество $\boldsymbol{K}^{\mathbf{o}} \in \boldsymbol{K}$) или иные операции по предварительному преобразованию (криптографическое шифрование, или помехоустойчивое кодирование сообщения M_i, или комбинация этих или иных методов, т. е, например, M_i преобразуется в M_{1i}) осаждаемого сообщения, а также по выбору элементов контейнера для такого осаждения: $\boldsymbol{K} = \{K_1, K_2, \ldots, K_z\}$.

Результатом прямых преобразований (составляют множество $\boldsymbol{F}$) будет стегоконтейнер S_q, относящийся ко множеству $\boldsymbol{S}$: $\boldsymbol{S} = \{S_1, S_2, \ldots, S_r\}$; соответствующие обратные преобразования составляют множество $\boldsymbol{F}^1$.

Введены понятия «*дополнительные стеганографические ключи*» и «*многоключевая стеганографическая система*».

Определение 1. *Дополнительный ключ первого рода* K_{w1} ($K_{w1} \in \boldsymbol{K}^{д1}$) стеганографической системы есть конкретное секретное значение из набора параметров алгоритма или нескольких алгоритмов, используемое для криптографического зашифрования, для помехоустойчивого кодирования или для иного метода предварительного преобразования сообщения M_i перед его осаждением. Расшифрование, декодирование или иная процедура при извлечении этого сообщения в общем случае зависит от ключа K^*_{w1} ($K^*_{w1} \in \boldsymbol{K}^{д1*}$); $K^*_{w1} \neq K_{w1}$ (неравенство справедливо, например, в случае использования асимметричного криптографического преобразования); $w_1 = 1, 2, \ldots, l_1$.

Определение 2. *Дополнительный ключ второго рода* K_{w2} ($K_{w2} \in \boldsymbol{K}^{д2}$) стеганографической системы есть конкретное секретное значение из набора параметров, используемое при определении цветовых, пространственных или иных параметров контейнера на каждом шаге осаждения сообщения M_{1i} или M_i (во втором случае ключ первого рода не используется в системе); $w_2 = 1, 2, \ldots, l_2$; $K^*_{w2} \in \boldsymbol{K}^{д2*}$.

Определение 3. *Многоключевой стеганографической системой* $\sum_{\boldsymbol{n}}$ называется совокупность множеств сообщений $\boldsymbol{M}$, контейнеров $\boldsymbol{C}$, основных ключей $\boldsymbol{K}^{о}$, дополнительных ключей $\boldsymbol{K}^{д}$ и $\boldsymbol{K}^{д*}$, стегосообщений $\boldsymbol{S}$ и преобразований (прямого $\boldsymbol{F}$ и обратного $\boldsymbol{F}^{1}$), которые их связывают:

$$\sum_{\boldsymbol{n}} = (\boldsymbol{M}, \boldsymbol{C}, \boldsymbol{K}, \boldsymbol{S}, \boldsymbol{F}, \boldsymbol{F}^{1}), \qquad (2)$$

где $\boldsymbol{K} = \{\boldsymbol{K}^{о}, \boldsymbol{K}^{д}, \boldsymbol{K}^{д*}\}$ и $\boldsymbol{K}^{д} = \{\boldsymbol{K}^{д1}, \boldsymbol{K}^{д2}\}$, $\boldsymbol{K}^{д*} = \{\boldsymbol{K}^{д1*}, \boldsymbol{K}^{д2*}\}$.

Основным отличием разработанной математической модели от известных является разделение используемой ключевой информации на три типа. Это позволит с большей точностью оценивать стойкость системы к взлому при использовании, например, вероятностных значений всех параметров модели: вероятностную оценку выбора ключевой информации, а также оценку стойкости системы к взлому или к модификациям можно будет осуществлять не по одному, а, по крайней мере, по трем независимым параметрам.

На рисунке 2 приведена обобщенная структурная схема стеганографической системы, синтезированная на основе разработанной модели, при условии выполнения некоторой фиксированной операции осаждения сообщения в соответствии с функцией F_w, $F_w \in \boldsymbol{F}$, и соответствующей операции извлечения — $(F^{-1})_w$, $(F^{-1})_w \in \boldsymbol{F}^{1}$.

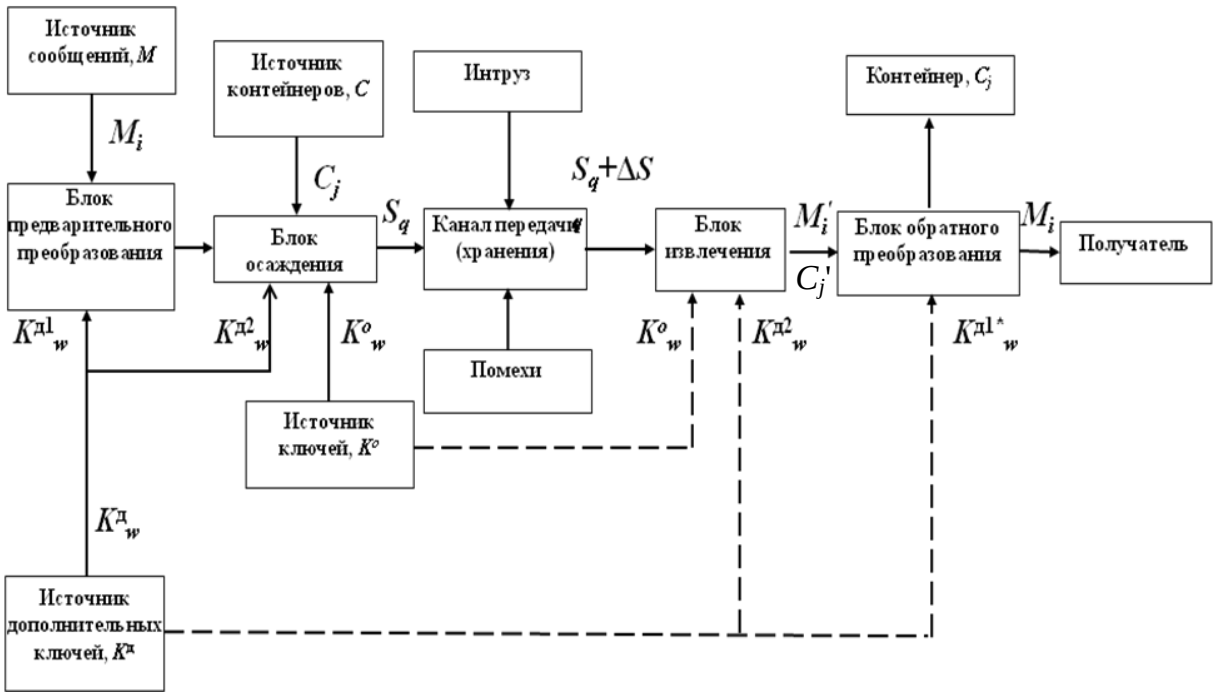

Рисунок 2. — Обобщенная структурная схема многоключевой стеганографической системы

Далее приводится обоснование необходимости использования для систем из области охраны прав интеллектуальной собственности двух параметров, относящихся к стеганостойкости: *стойкость стегоконтейнера к взлому* (обнаружение и извлечение сообщения) и *стойкость к нарушению целостности стегоконтейнера*.

Основой для анализа стойкости стегоконтейнера к взлому могут служить условные вероятности размещения в конкретно выбранном стегоконтейнере S_q сообщений M_i ($M_i \in M$):

$$P_{M|S_q} = \{P(M_1|S_q), P(M_2|S_q), \ldots, P(M_n|S_q)\} \qquad (3)$$

и аналогичным образом рассчитанные условные вероятности использования различных ключей при осаждении и извлечении информации: $P_{К^o|S_q}$, $P_{К^{д1}|S_q}$($P_{К^{д1*}|S_q}$), $P_{К^{д2}|S_q}$. Указанные множества условных вероятностей образуют совокупность предварительных сведений для извлечения из стегоконтейнера осажденного сообщения другим лицом.

Задача оценки стойкости системы — в виде текстового документа с осажденной информацией к взлому — приобретает свойственную таким системам специфику: важен не столько факт извлечения злоумышленником сообщения M_i из стегоконтейнера S_q, сколько обеспечение це-

лостности стегоконтейнера при умышленном или случайном воздействии на него (обозначается формально ΔS_q).

Для формального описания процессов осаждения/извлечения сообщения M_i на основе модификации цветовых или пространственных параметров (апрош или кернинг) текста-контейнера предложено использовать известный подход на основе *горизонтальных* и *вертикальных профилей* выделенного фрагмента текста.

Определение 4. *Профилем* называется проекция массива A пикселей или фрагмента этого массива, значения элементов которых определены дискретной функцией $f(x, y) \in \{0, 1\}$ для $1 \le x \le W$и $1 \le y \le L$, на одну из осей — x или y.

Отдельная строка или фрагмент текста представляется функцией $f(x, y)$, которая определяет координату для каждого пикселя изображения в двумерном пространстве (или массиве) A; в общем случае $x = 1, 2, \ldots, W$, W — количество «черных» (или в координатах модели *RGB*) пикселей в одном горизонтальном ряду черно-белого (или *RGB*) растра, формирующего анализируемый фрагмент текста); $y = 1, 2, \ldots, L$, L — количество «черных» (или иного цвета) пикселей в одном вертикальном ряду такого растра.

Выражения для нахождения численных значений горизонтального (H) и вертикального (V) профилей (соответствующих гистограмм) имеют вид:

$$H(x,y) = \sum_{x=1}^{W} f(x,y), \qquad V(x,y) = \sum_{y=1}^{L} f(x,y) \tag{4}$$

В **третьей главе** рассмотрена сущность предлагаемых синтаксических методов текстовой стеганографии, основанных на использовании пространственно-геометрических (таких, как апрош, кернинг) и цветовых параметров символов текста, формируемого растром. Здесь же приведены и описаны алгоритмы, реализующие разработанные методы.

Модификация указанных параметров текста позволяет осаждать тайное сообщение (авторскую информацию) в процессе прямого стеганографического преобразования защищаемого текста-контейнера либо передавать эту информацию по стегоканалу. В первом случае решается задача защиты права интеллектуальной собственности, во втором — обеспечения повышенного уровня конфиденциальности передаваемых сообщений между абонентами в соответствии с рисунком 2.

Разработано математическое обеспечение предложенных стеганографических методов. В основе математического описания *метода на ос-*

нове модификации цвета Φ символа текста лежит известная *RGB*-модель представления цветовых координат пикселей, формирующих текст, который мы отождествляем с изображением:

$$\Phi = rR + gG + bB, \quad (5)$$

где R,G,B — постоянные, линейно независимые (основные) цвета: соответственно красный, зеленый и синий; r, g, b — количественные (весовые) коэффициенты в выбранной шкале.

Предложено кодировать данные (относящиеся к M_i) с помощью изменения исходного цвета определенных символов текстового документа, C_j. Отклоняя значение базового (исходного) цвета в ту или иную сторону, можно скрыть необходимую информацию.

Оригинальность метода состоит в том, что процессы осаждения/извлечения информации осуществляются при сравнительном изменении/анализе цветовых параметров пар соседних символов: $\{r_t, g_t, b_t\}$ и $\{r_{t+1}, g_{t+1}, b_{t+1}\}$. При этом цветовые координаты $\{r_t, g_t, b_t\}$ являются базой для осаждения/извлечения определенного знака («0» или «1») сообщения. Изменение параметра соседнего символа оценивается по отношению к этому базовому: цвет пикселей, формирующих символы текста-контейнера, можно изменить так, что это остается незаметным для других лиц в силу специфики человеческого зрения. Это справедливо и для методов, направленных на модификацию пространственно-геометрических параметров текста.

Алгоритм реализации метода состоит из следующих операций.

Шаг 1. Определение текстового документа-контейнера.

Шаг 2. Выбор сообщения, которое необходимо скрыть (M_i). Выбор основного ключа. Выбор дополнительных ключей первого рода (при необходимости).

Шаг 3. Подсчет общего количества знаков Z в документе-контейнере (C_j).

Шаг 4. Представление сообщения M_i в двоичном виде.

Шаг 5. Предварительное шифрование и/или кодирование сообщения M_i с помощью ключевой информации первого рода ($K^{д1}$ — при необходимости).

Шаг 6. Подсчет общего числа N знаков, составляющих стегосообщение M_i.

Шаг 7. Проверка условия: $Z \geq N$? При выполнении условия — переход к шагу 8, в противном случае — к шагу 2.

Шаг 8. Выбор ключей второго рода.

Шаг 9. Выбор текущего t-го символа документа-контейнера C_j в соответствии с ключом $(K^{д21})_{w21}$.

Шаг 10. Осаждение очередного двоичного символа или символов сообщения, сформированного на шаге 5, в (t+1)-й символ контейнера с использованием ключа $(K^{д22})_{w22}$.

Шаг 11. Проверка условия: $t+1 < N$? При выполнении условия — переход к шагу 9, в противном случае — к шагу 12.

Шаг 12. Конец.

Алгоритм извлечения сообщения M_i из выбранного S_q при известных автору сообщения значениях ключевой информации, в основном, предусматривает выполнение операций, обратных по отношению к операции на шаге 10 при учете условий на ш. 9 и ш. 11 приведенного алгоритма осаждения.

Метод на основе модификации апроша. Встраивание стегосообщения основано на модификации базового (устанавливаемого текстовым процессором по умолчанию) значения апроша, a_o, его изменением от базового до некоторого максимального $a_{\max}$ (или минимального, $a_{\min}$) значения. Такое изменение производится с определенным шагом (дискретно) Δa_t, каждому значению которого присваивается определенный бит или определенная комбинация бит осаждаемого сообщения.

Изменение величины апроша между определенными символами (первый из них — t-й) текста C_j относительно базового значения a_o на небольшое расстояние (пункты (пт) или доли пункта) представляем в виде:

$$a_t' = a_o + \Delta a_t. \qquad (6)$$

Такое изменение не должно вызывать визуально заметного уплотнения ($\Delta a_t < 0$) или разрежения ($\Delta a_t > 0$) групп символов.

Основная особенность — в текстовом процессоре MS Word апрош может принимать значения в диапазоне от 0 до 1584 пунктов (пт), а апрош можно изменять дискретно с интервалом 0,1 пт. Это дает возможность осаждать в контейнере объемы сообщений, многократно превосходящие возможности известных методов. Алгоритм реализации данного метода во многом схож с алгоритмом реализации метода на основе модификации цвета. Основное отличие — операция на ш. 10 предусматривает модифи-

кацию апроша t-го символа, выбранного на ш. 9. Встраиваемая при этом информация определяется параметром Δa_t, который соответствует ключу $(K^{д22})_{w22}$. Кроме того, на шаге 6 подсчитывается число бит N_{2c} в осаждаемом сообщении, а на шаге 11 проверяется иное условие: $t < N_{2c}$?

Метод на основе модификации кернинга. Основывается на принудительном применении кернинга (изменении межсимвольного расстояния) к специфическим парам знаков (кернинговым парам), не зависящем от установок параметров текста-контейнера. В MS Word кернинг применяется к символам, размер (кегль) которых не ниже заданного специальной опцией в диапазоне от 1 до 1638 пт. Такая опция может применяться независимо к любым парам знаков и даже единичным знакам текста. Разработаны и описаны два варианта практической реализации метода.

Вариант 1. Предполагает осаждение в одной кернинговой паре одного бита сообщения, переведенного в двоичный вид при соответствующем объеме N_{2c}: например, «0», если кернинг для этой пары не применяется, и «1» — если применяется. Основывается на том, что автоматически установленный кернинг в виде определенного межсимвольного расстояния ($\Delta\sigma$) для шрифта с установленным размером (кеглем) Em не будет применяться процессором по отношению к любым парам символов меньшего размера ($Em - (\Delta_{Em})$). Отклонение размера $(Em)_t$ некоторой t-й кернинговой пары символов на величину Δ_{Em} от установленной Em означает, что в ней осажден «0» (кернинга нет) и «1» — в противном случае. При этом максимальный объем (бит) осажденного сообщения в анализируемом варианте не может превысить числа выявленных кернинговых пар в тексте-контейнере. При этом

$$\Delta\sigma_t = 0, \text{при } Em - (Em)_t = \Delta_{Em}; \Delta\sigma_t \neq 0, \text{ при } Em - (Em)_t = 0, \qquad (7)$$

где $t = 1, 2, \ldots, Z_k$, Z_k — количество кернинговых пар в документе-контейнере C_j.

Вариант 2. Отличается от предыдущего способом кодирования осаждаемого сообщения. Сам факт применения или неприменения кернинга значения не имеет, как не имеет значения и размер шрифта документа. Имеет значение лишь указанный для произвольной (t-й) кернинговой пары текста-контейнера параметр $(Em)_t$, который может выбираться из указанного выше диапазона. При этом

$$(Em)_t = k_e^{д22},\ k_e^{д22} \in (K^{д22})_{w22}, \qquad (8)$$

$t = 1, 2, \ldots, Z_k$, $e = 1, 2, \ldots, 1024$.

Данный вариант предусматривает возможность осаждения в одной кернинговой паре до 10 бит сообщения. В сравнении с алгоритмами осаждения информации для двух предыдущих методов алгоритм реализации данного метода предусматривает на ш. 3 подсчет Z_k и индексирование каждой кернинговой пары, а также использование Z_k в операциях сравнения на ш. 7.

Вычислительная сложность всех алгоритмов зависит линейно от объема осаждаемой информации, т. е. алгоритмы относятся к классу сложности $O(n)$.

В **четвертой главе** для оценки эффективности и стеганографической стойкости предложенных в работе синтаксических методов описаны созданные программные средства, не имеющие аналогов в странах СНГ и зарегистрированные в Национальном центре интеллектуальной собственности Республики Беларусь.

Выполнена оценка эффективности разработанных методов, количественным выражением которой предложено использовать показатель *плотности заполнения пустого контейнера* C_j символами осаждаемого сообщения M_i. Разработана методика экспериментального определения параметра эффективности, которая сводится к выполнению следующих операций:

1) выбор инструментальной базы эксперимента (указанные программные средства);

2) выбор символов текста-контейнера (стегознаков), которые могут быть использованы для осаждения информации каждым из анализируемых методов;

3) формирование информационной базы эксперимента — множество пустых контейнеров (в нашем случае — в виде 40 литературных источников в цифровой форме общим объемом в несколько Гигабайт);

4) выполнение процедуры осаждения сообщения M_i на основе каждого из методов в каждый пустой контейнер;

5) обработка и анализ полученных результатов.

Установлено, все предложенные в диссертационной работе методы по эффективности использования объема текста-контейнера для осаждения тайного сообщения превосходят все известные синтаксические методы на 20–90 %.

Изучены и проанализированы два аспекта оценки стойкости методов:

1) к выявлению видимых (на основе визуального анализа) отклонений цветовых и пространственно-геометрических параметров текста-контейнера с осажденной информацией от общепринятого формата;

2) к случайным или преднамеренным изменениям указанных параметров, которые происходят при переформатировании стегоконтейнера (например, изменением кегля или переводом текста в другой формат).

По п. 1. Эксперименты (опрос респондентов — школьники и студенты — после визуального изучения ими параметров шрифта представленного текста) выявили хорошую стойкость методов осаждения до 4 бит информации на один символ текста-контейнера на основе модификации цветовых и пространственно-геометрических параметров символов текста к визуальному анализу. Указанная верхняя граница (4 бита) в 2–4 раза превышает аналогичный показатель для всех известных синтаксических методов текстовой стеганографии.

По п. 2. Из числа разработанных методов установлена абсолютная стойкость для метода на основе модификации цветовых параметров по отношению к конвертации стегоконтейнера по схеме «*.docx — *.pdf. — *.docx». Установлено также, что межсимвольное расстояние (конкретно — апрош) при указанном типе трансформации стегоконтейнера приводит к потере (частичной) осажденной информации ($\Delta S_q > 0$). Перевод документа на другой шрифт (например, с Arial на Times New Roman) не приводит к изменению осажденной информации для методов на основе модификации цвета и апроша ($\Delta S_q = 0$), однако может приводить к частичной ее потере для метода на основе кернинга, с учетом того, что «внутри» MS Word разным шрифтам соответствуют различные таблицы кернинговых пар.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Совокупность выдвинутых и обоснованных в диссертационной работе положений, полученных научных и практических результатов позволяет на новом, более эффективном уровне решать актуальную, относящуюся к одному из приоритетных направлений научно-технической деятельности в Республике Беларусь, задачу — защиты прав интеллектуальной собственности на электронные текстовые документы.

Основным результатом диссертационного исследования является разработка и анализ новых оригинальных методов и инструментальных

средств текстовой стеганографии, основанных на модификации цветовых и пространственно-геометрических параметров символов текстовых документов и предоставляющих дополнительные возможности для повышения эффективности решения задач по защите авторского права в ИТ-отрасли.

В диссертации получены следующие теоретические и практические результаты:

1. Обоснована и сформулирована концепция нового типа универсальной стеганографической системы, которая классифицирована как многоключевая. Основным ее отличием от известных стегосистем является разделение используемой ключевой информации (КИ) на три типа: основную, определяющую базовый метод осаждения (или извлечения) тайного сообщения, и два типа дополнительной ключевой информации: КИ первого рода, относящуюся к методам предварительного преобразования сообщения (до его осаждения), и КИ второго рода, относящуюся к порядку размещения элементов осаждаемого сообщения среди элементов документа для защиты права интеллектуальной собственности на него. Это позволило создать математическую модель стеганографической системы с большей степенью адекватности, определить понятные логические связи между информационными процессами, происходящими в такой системе, и структурой самой системы [2–5, 30, 31, 34, 35].

2. Разработана математическая модель многоключевой стеганографической системы. Основой модели является теоретико-множественное определение и взаимозависимость основных компонент системы, представляющей собой совокупность множеств сообщений, контейнеров, основных ключей, дополнительных ключей первого рода, дополнительных ключей второго рода, стегоконтейнеров (заполненных контейнеров) и преобразований (прямого — осаждение, и обратного — извлечение сообщения), которые их связывают. Основным отличием модели от известных является более высокая степень адекватности, достигаемая увеличением числа существенных параметров модели в виде дополнительных ключей. На основе математической модели синтезирована структурная схема многоключевой стеганографической системы. Исследованы особенности системы для ее использования при решении задач на основе текстовой стеганографии [4, 5, 30, 31, 34, 35].

3. Предложен и исследован подход к анализу и оценке стойкости системы текстовой стеганографии. Обоснована необходимость и целесообразность использования для систем такого назначения двух параметров: стой-

кость стегоконтейнера (защищаемого документа с осажденным тайным сообщением) к взлому (обнаружение и извлечение сообщения) и устойчивость к нарушению целостности стегоконтейнера. Отличием такого подхода является то, что для анализа первого из указанных видов стойкости предложено использовать множества условных вероятностей, которые определяют формирование конкретного стегоконтейнера при условиях использования конкретных компонент стеганографической системы, выбранных из соответствующего множества в соответствии с п. 2 заключения, целостность же стегоконтейнера определяется устойчивостью к искажениям, которые вносятся в процессе его конвертации [3, 22, 23, 28, 32].

4. Разработан новый подкласс синтаксических методов текстовой стеганографии, в основе которого лежит идея модификации цветовых параметров символов текста-контейнера и пространственно-геометрических параметров шрифтов (апрош, кернинг) при осаждении/извлечении тайного сообщения. При этом для извлечения сообщения могут быть использованы вертикальные и горизонтальные профили пикселей, формирующих растровое изображение текста. Разработано математическое обеспечение и алгоритмы реализации (относятся к классу сложности $O(n)$) всех предложенных методов [6, 7, 8, 16, 18, 19,21, 22, 26, 28, 32–34, 36].

5. Разработаны методики оценки эффективности и стеганографической стойкости разработанных методов к визуальному анализу, устойчивости к преднамеренным или случайным модификациям содержания защищаемого документа. Количественным выражением эффективности предложено использовать показатель плотности заполнения пустого контейнера символами осаждаемого сообщения. По этому параметру предложенные методы превосходят все известные синтаксические методы на 20–90 %. Экспериментально доказано, что стеганографическая стойкость методов к визуальному анализу стегоконтейнера, направленному на выявление самого факта наличия осажденного сообщения, находится на уровне размещения 3-х бит (для метода на основе апроша), 10 бит (для метода на основе кернинга) тайного сообщения на один символ текста и на уровне 10–12 бит (для метода на основе модификация цвета). Указанная верхняя граница в 2–4 раза превышает аналогичный показатель для известных синтаксических методов текстовой стеганографии, для которых существует физическое ограничение в объеме осаждаемой информации на символ, равное 1–2 битам. Указанные количественные оценки позволили сформировать показатели качества методов текстовой стеганографии [1, 7, 13, 15–17, 20, 23, 29].

6. Разработаны и зарегистрированы в Национальном центре интеллектуальной собственности Республики Беларусь программные средства на основе предложенных в работе синтаксических методов текстовой стеганографии. Средства являются импортозамещающими для страны [1, 10, 13, 27, 37–39].

Рекомендации по практическому использованию результатов

Результаты работы получены и реализованы в рамках госбюджетных НИР: ГБ 11-165, ГБ 11-025, ГБ 14-167, ГБ 16-113, выполненных на кафедре информационных систем и технологий УО «Белорусский государственный технологический университет».

На основе предложенных в работе решений могут быть сформулированы следующие рекомендации:

1. Разработанная универсальная многоключевая стеганографическая система может быть использована не только для защиты права интеллектуальной собственности, но и для тайной передачи сообщений.

2. Предложенная в работе новая концепция текстовой стеганографии, основанная на модификации цветовых и пространственно-геометрических параметров защищаемого текста, может служить методической и информационной основой для расширения и углубления исследований по решению прикладных задач в предметной области, например, при защите контента электронных образовательных средств.

3. Разработанные и зарегистрированные в Национальном центре интеллектуальной собственности Республики Беларусь программные средства могут быть использованы не только для защиты прав собственности на текстовые документы, но также для более глубокого анализа и исследования предложенных и похожих методов.

Результаты диссертационной работы внедрены и используются (акты приведены в приложении 2):

1. В унитарном предприятии «Инфотех» (Минск) при разработке программного модуля «Криптошифр».

2. В учебном процессе УО «Белорусский государственный технологический университет».

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых журналах

1. Urbanovich, P. Text steganography application for protection and transfer of the information / P. Urbanovich, N. Urbanovich[1], K. Chourikov, A. Rimorev // Electrical Review (Przeglad elektrotechniczny). — 2010. — № 7. — P. 95–97.

2. Urbanovich, N. The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // Electrical Review (Przeglad elektrotechniczny). — 2012. — № 11b. — P. 342–344.

3. Шутько, Н. П. Защита авторских прав на электронные текстовые документы методами стеганографии / Н. П. Шутько // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. — 2013. — Вып. 6 — С. 131–134.

4. Шутько, Н. П. Особенности и формальное описание процесса осаждения секретной информации в текстовые документы на основе стеганографии / Н. П. Шутько // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. — 2014. — Вып.6. — С. 121–124.

5. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. — 2015. — № 6. — С. 152–156.

6. Шутько, Н. П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста / Н. П. Шутько // Труды БГТУ. Сер. VI: Физ.-мат. наук и иинформатика. — 2016. — Вып. 6. — С. 160–165.

7. Shutko, N. The use of aprosh and kerning in text steganography / N. Shutko // Electrical Review (Przeglad elektrotechniczny). — 2016. — № 10. — P. 222–225.

Материалы конференций

8. Урбанович, Н. П.[2] Стеганографические методы скрытия информации в тексте / Н. П. Урбанович, Т. В. Коваленок // Материалы XII Республиканской научной конференции студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и в научных исследованиях», апрель, 2009 г. — Гомель: ГГУ. — С. 168–169.

[1]Девичья фамилия Н.П. Шутько
[2]Девичья фамилия Н.П. Шутько

9. Коваленок, Т. В. Стеганографические методы скрытия информации в неподвижных изображениях / Т. В. Коваленок, Н. П. Урбанович // Материалы XII Республиканской научной конференции студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и в научных исследованиях»: апрель, 2009 г. — Гомель: ГГУ. — С. 30–31.

10. Urbanovich, P. P. Text steganography application for protection and transfer of the information / P. P. Urbanovich, K. V. Chourikov, A. V. Rimarev, N. P. Urbanovich // Proc. of the 6-th Intern. Conf. on New Electrical and Electronic Technologies and their Industrial Implementation, Zakopane, Poland, 23–26.06. 2009. — 2009. — P. 60–61.

11. Урбанович, Н. П. Сравнительный анализ методов текстовой стеганографии / Н. П. Урбанович, Т. В. Коваленок // 60-я научно-техническая конференция студентов и магистрантов БГТУ: сб. научных работ в 4 ч. — Ч. 4. —Минск: БГТУ. — 2009. — С. 111–115.

12. Коваленок, Т. В. Сравнительная характеристика методов скрытия информации в графических объектах / Т. В. Коваленок, Н. П. Урбанович // 60-я научно-техническая конференция студентов и магистрантов БГТУ: сб. научных работ в 4 ч. — Ч. 4. — Минск: БГТУ. — 2009. — С. 108–111.

13. Урбанович, П. П. Применение текстовой стеганографии для защиты и передачи информации / П. П. Урбанович, Н. П. Урбанович, А. В. Риморев, Т. В. Коваленок // Международная научно-техническая конференция «Автоматический контроль и автоматизация производственных процессов». Сборник материалов. — Минск: БГТУ. — 2009. — С. 67–69.

14. Урбанович, П. П. Стеганография в графических объектах / П. П. Урбанович, Т. В. Коваленок, Н. П. Урбанович// МНТК «Автоматический контроль и автоматизация производственных процессов». Сборник материалов. — Минск: БГТУ. — 2009. — С. 69–71.

15. Urbanovich, N. The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // Proc. of the 7-th Intern. Conf. on New Electrical and Electronic Technologies and their Industrial Implementation, Zakopane, Poland, 28.06–01.07.2011. — 2011. — P. 147–148.

16. Urbanovich, N. Development, analysis of efficiency and performance in an electronic textbook methods of text steganography / N. Urbanovich // Printing future days: 4th International Scientific Conference on Printing and Media Technology. Proceedings, Chemnitz, Germany, 07–10.11.2011. — P. 189–193.

17. Урбанович, Н. П. Исследование эффективности стеганографиче-

ских методов скрытия информации в тексте / Н. П. Урбанович // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы XIII Республиканской научной конференции студентов и аспирантов (Гомель, 21-23 марта 2011 г.). — Ч. 2. — Гомель: ГГУ им. Ф. Скорины, 2011. — С. 27–28.

18. Коваленок, Т. В. Идентификация стегоизображения на основе оценки показателя яркости / Т. В. Коваленок, Н. П. Урбанович // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы XIII Республиканской научной конференции студентов и аспирантов (Гомель, 21-23 марта 2011 г.). — Ч. 2. — Гомель: ГГУ им. Ф. Скорины, 2011. — С. 21–22.

19. Пласковицкий, В. А. Управление защитой информации на основе стеганографических методов / В. А. Пласковицкий, Н. П. Шутько // Международная научно-техническая конференция «Автоматический контроль и автоматизация производственных процессов». Сб. материалов. — Минск: БГТУ, 2012. — С. 283–285.

20. Пласковицкий, В. А. Защита авторских прав на программные средства и текстовые документы с помощью специальных методов / В. А. Пласковицкий, Н. П. Шутько, П. П. Урбанович // Информационные технологии и системы 2012 (ИТС 2012): материалы международной научной конференции, БГУИР, Минск, Беларусь, 24 октября 2012 г. = Information Technologies and Systems 2012 (ITS 2012): Proceeding of The International Conference, BSUIR, Minsk, 24th October 2012 / редкол.: Л. Ю. Шилин [и др.]. — Минск: БГУИР, 2012. — С. 242–243.

21. Шутько, Н. П. Использование стеганографических методов для защиты прав интеллектуальной собственности / Н. П. Шутько // Сборник научных работ 64-ой НТК студентов и магистрантов БГТУ, 22–27 апреля 2013. — Минск, БГТУ. — Ч3. — 2013. — С. 272–275.

Тезисы докладов

22. Урбанович, Н. Использование параметров символов документов процессора MSWord в текстовой стеганографии / Н. Урбанович, Т. Коваленок, А. Риморев // 10-ї МНТК студентів і аспірантів «Друкарство молоде»: тези доповідей. — Київ: НТУУ КПИ, 2010. — Кн. 1. — С. 134–135.

23. Коваленок, Т. Устойчивость к визуальным атакам в LSB-стегосистемах / Т. Коваленок, Н. Урбанович, Ю. Мурашко // 10-ї МНТК студентів і аспірантів «Друкарство молоде»: тези доповідей. — Київ: НТУУ КПИ, 2010. — Кн. 1. — С. 159–161.

24. Урбанович, Н. П. Защита информации методами текстовой стеганографии / Н. П. Урбанович, Т. В. Коваленок // тези доповідей: II міжнародної НТК студентів і аспірантів «Кваліlогія книгі». — Львів, 2010. — С. 156–157.

25. Коваленок, Т. В. Технология защиты изображений посредством LSB-стегосистемы / Т. В. Коваленок Н. П. Урбанович // тези доповідей: II міжнародної НТК студентів і аспірантів «Кваліlогія книгі». — Львів, 2010. — С. 158–159.

26. Урбанович, Н. Использование синтаксического метода текстовой стеганографии на основе изменения апроша / Н. Урбанович, Т. Коваленок // тези доповідей: 11-ї МНТК студентів і аспірантів «Друкарство молоде». — Київ: НТУУ КПИ, 2011. — Кн. 1. — С. 141–142.

27. Урбанович, Н. Создание электронного учебника на тему «текстовая стеганография» / Н. Урбанович // Международная конференция молодых ученых Print–2011: тезисы докладов. — СПб.: Петерб. ин-т печати, 2011. — С. 144–145.

28. Урбанович, Н. П. Стеганографическая защита текстовой информации путем изменения цветовых характеристик символа / Н. П. Урбанович, В. А. Пласковицкий // Сборник тезисов докладов Республиканской научной конференции студентов и аспирантов Республики Беларусь «НИРС–2011». — Минск: Издательский центр БГУ, 2011. — С. 368.

29. Shutko, N. Text steganography as an effective instrument of protection of the copyright on electronic document / N. Shutko // Proc. of 8-th Int. Conf. on New Electrical and Electronic Technologies and their Industrial Implementation, NEET'2013, Zakopane, Poland, 18-21.06.2013. — 2013. — P. 147.

30. Шутько, Н. П. Математическое моделирование процесса встраивания авторской информации в текстовые документы методами стеганографии / Н. П. Шутько, В. А. Пласковицкий // Микроэлектроника и информатика-2014: 21-я Всероссийская межвузовская н.-технич. конф. студ. и аспирантов, Зеленоград, 23-25 апреля 2014. — М.: МИЭТ, 2014. — С. 213.

31. Шутько, Н. П. Формальное описание процесса осаждения секретной информации в текстовые документы на основе стеганографии / Н. П. Шутько // Издательское дело и полиграфия, 78-я науч.-технич. конф. проф.-препод. состава, науч. сотрудников и аспирантов, (с междунар. участ.), Минск, 3–13.02.2014 [Электронный ресурс]. — Минск: БГТУ, 2014. — С. 37.

32. Shutko, N. The use of aprosh and kerning in text steganography / N. Shutko, E. Blinova // Proc. of 9-th Int. Conf. on New Electrical and Electronic

Technologies and their Industrial Implementation, NEET'2015, Poland, 23–26.06.2015. — 2015. — P. 77.

33. Shutko, N. Text steganography method based on the change of font attributes / N. Shutko // Printing future days: 6th International Scientific Conference on Printing and Media Technology, Proceedings. — Germany, Chemnitz, 8–9.10.2015. — P. 91.

34. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Информационные технологии: тезисы 79-й НТК проф.-преп. состава, научн. сотр. и аспирантов (с междунар. участ.), Минск, 2–6.02.2015 [Электронный ресурс]. — Минск: БГТУ, 2015. — С. 14−15.

35. Шутько, Н. П. Моделирование стеганографической системы в задачах по охране авторских прав / Н. П. Шутько, Н. И. Листопад, П. П. Урбанович // 8-я МНТК Информационные технологии в промышленности, ITI–2015. Тезисы докладов, Минск, 2–3.04.2015. — Минск: ОИПИ НАНБ, 2015. — С. 30–31.

36. Шутько, Н. П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста/ Н.П. Шутько// Информационные технологии: тезисы 80-й НТК проф.-преп. состава, научн. сотр. и аспирантов (с междунар. участ.), Минск, 1–16.02.2016 [Электронный ресурс]. — Минск: БГТУ, 2016. — С.19.

Свидетельства о регистрации компьютерных программ

37. Свидетельство о регистрации компьютерной программы «Sword» / В. А. Пласковицкий, Н. П. Шутько// Реестр Национального Центра интеллектуальной собственности Республики Беларусь. — 2012. — Запись № 383 от 04.01.2012.

38. Свидетельство о регистрации компьютерной программы «KSteg» / А. В. Щербацкий, Н. П. Шутько // Реестр Национального Центра интеллектуальной собственности Республики Беларусь. — 2014. — Запись № 628 от 10.01.2014.

39. Свидетельство о регистрации компьютерной программы«MathCrypto 1.0» / В. А. Пласковицкий, П. П. Урбанович, Н. П. Шутько// Реестр Национального Центра интеллектуальной собственности Республики Беларусь. — 2014. — Запись № 717 от 15.12.2014.

РЕЗЮМЕ

Шутько Надежда Павловна

ЗАЩИТА ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ НА ТЕКСТОВЫЕ ДОКУМЕНТЫ МЕТОДАМИ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Ключевые слова: интеллектуальная собственность, стеганография, параметры шрифта, профиль текста, математическая модель, алгоритм.

Цель работы: разработка и анализ эффективных методов и инструментальных средств текстовой стеганографии, основанных на модификации цветовых и пространственно-геометрических параметров символов текста, для решения задач по обеспечению авторского права на электронные текстовые документы.

Методы исследований: носят теоретический и экспериментальный характер; базируются на основе теории информационных процессов и систем, теории множеств, теории вероятностей и математической статистики, теории шрифтов; постановка имитационных экспериментов базируется на использовании специализированных компьютерных программных средств.

Полученные результаты и их новизна.

В основу разработанных стеганографических методов, реализующих их алгоритмов и необходимого математического обеспечения положена идея использования цветовых и пространственно-геометрических параметров символов защищаемого текста (апрош, кернинг), модификация которых позволяет осаждать/извлекать тайную информацию, предназначенную для защиты прав интеллектуальной собственности.

Обоснован и исследован новый подкласс стеганографических систем, определенный как «многоключевые стеганографические системы». Методика оценки эффективности разработанных и известных методов текстовой стеганографии основана на использовании и анализе введенного показателя «плотности заполнения стегоконтейнера» символами тайного сообщения.

Область применения.

Разработанная универсальная многоключевая стеганографическая система может быть использована не только для защиты права интеллектуальной собственности, но и для тайной передачи сообщений.

Предложенная в работе новая концепция текстовой стеганографии, основанная на модификации цветовых и пространственно-геометрических параметров защищаемого текста, может служить методической и информационной основой для расширения и углубления исследований по решению прикладных задач в предметной области, например, при защите контента электронных образовательных средств.

РЭЗЮМЭ

Шуцько Надзея Паўлаўна

АХОВА ПРАВОЎ ІНТЭЛЕКТУАЛЬНАЙ УЛАСНАСЦІ НА ТЭКСТАВЫЯ ДАКУМЕНТЫ МЕТАДАМІ КАМП'ЮТАРНАЙСТЭГАНАГРАФІІ

Ключавыя словы: інтэлектуальная ўласнасць, стэганаграфія, параметры шрыфту, профіль тэксту, матэматычная мадэль, алгарытм.

Мэта працы: распрацоўка і аналіз эфектыўных метадаў і інструментальных сродкаў тэкставай стэганаграфіі, заснаваных на мадыфікацыі колеравых і прасторава-геаметрычных параметраў сімвалаў тэксту, для вырашэння задач па забеспячэнні аўтарскага права на электронныя тэкставыя дакументы.

Метады даследаванняў: носяць тэарэтычны і эксперыментальны характар; базіруюцца на аснове тэорыі інфармацыйных працэсаў і сістэм, тэорыі мностваў, тэорыі верагоднасцяў і матэматычнай статыстыкі, тэорыі шрыфтоў; пастаноўка імітацыйных эксперыментаў заснавана на выкарыстанні спецыялізаваных камп'ютарных праграмных сродкаў.

Атрыманыя вынікі і іх навізна.

У аснову распрацаваных стэганаграфічных метадаў, алгарытмаў, якія іх рэалізуюць, і неабходнага матэматычнага забеспячэння пакладзена ідэя выкарыстання колеравых і прасторава-геаметрычных параметраў сімвалаў ахоўваемага тэксту (апрош, кернінг), мадыфікацыя якіх дазваляе асаджаць/ здабываць сакрэтную інфармацыю, прызначаную для аховы правоў інтэлектуальнай уласнасці.

Абгрунтаваны і даследаваны новы падклас стэганаграфічных сістэм, азначаны як «многаключавыя стэганаграфічныя сістэмы». Методыка ацэнкі эфектыўнасці распрацаваных і вядомых метадаў тэкставай стэганаграфіі заснавана на выкарыстанні і аналізе ўведзенага паказчыка «шчыльнасці запаўнення стэгакантэйнера» сімваламі тайнага паведамлення

Вобласць прымянення.

Распрацаваная універсальная многаключавая стэганаграфічная сістэма можа быць выкарыстана не толькі для аховы права інтэлектуальнай уласнасці, але і для таемнай перадачы паведамленняў.

Прапанаваная ў працы новая канцэпцыя тэкставай стэганаграфіі, заснаваная на мадыфікацыі колеравых і прасторава-геаметрычных параметраў ахоўваемага тэксту, можа служыць метадычнай і інфармацыйнай асновай для пашырэння і паглыблення даследаванняў па рашэнні прыкладных задач у прадметнай вобласці, напрыклад, пры ахове кантэнту электронных адукацыйных сродкаў.

SUMMARY

Nadzeya Paulauna Shutko

PROTECTION OF THE INTELLECTUAL PROPERTY RIGHTS ON THE TEXT DOCUMENTS BY THE METHODS OF COMPUTER STEGANOGRAPHY

Keywords: intellectual property, steganography, font settings, profile of the text, mathematical model, algorithm.

Objective: the development and analysis of effective methods and tools of text steganography based on the modification of the color and dimensionally-geometrical parameters of the text characters to solve the problems of ensuring the copyright on the electronic text documents.

Research methods: methods have theoretical and experimental character; they are based on the theory of information processes and systems, the theory of sets, the theory of probability and mathematical statistics, theory of fonts; a carrying out of the simulations is based on the use of specialized computer software.

The obtained results and their novelty.

The basis of the developed steganographic methods, algorithms, that realize them, and the necessary mathematical software is the idea of the use of color and dimensionally-geometrical parameters of the characters in protected text (aprosh, kerning), modification of which allows to embed/extract secret information for the protection of intellectual property rights.

The new subclass of the steganographic systems defined as «multikey steganographic systems» is reasonable and investigated. The methodology to evaluate the efficiency of developed and known methods of a text steganography is based on the use and the analysis of the entered parameter of «density of a stego-container filling » with symbols of the secret message.

Application area.

The developed universal multikey steganographic system can be used not only for protection of the intellectual property right, but also for secret transmission of messages.

The new concept of a text steganography is on the modifications of color and dimensionally-geometrical parameters of the securable text can be used like a methodical and information basis for extension and a dimple of researches on the solution of application-oriented tasks in subject domain, for example, in case of protection of the content of electronic educational resources.