

ГОСУДАРСТВЕННОЕ НАУЧНОЕ УЧРЕЖДЕНИЕ
«ОБЪЕДИНЕННЫЙ ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК БЕЛАРУСИ»

Объект авторского права

УДК 003.26+347.78

БЛИНОВА
Евгения Александровна

**СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ И АЛГОРИТМЫ
ЗАЩИТЫ АВТОРСКОГО ПРАВА И ОБЕСПЕЧЕНИЯ
ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ
НА ОСНОВЕ ЯЗЫКОВ РАЗМЕТКИ**

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук
по специальности 05.25.05 – информационные системы и процессы

Минск 2024

Научная работа выполнена в учреждении образования «Белорусский государственный технологический университет».

Научный руководитель **Урбанович Павел Павлович**, доктор технических наук, профессор, профессор кафедры информационных систем и технологий Белорусского государственного технологического университета

Официальные оппоненты: **Листопад Николай Измаилович**, доктор технических наук, профессор, заведующий кафедрой информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники

Садов Василий Сергеевич, кандидат технических наук, доцент, профессор кафедры интеллектуальных систем Белорусского государственного университета

Оппонирующая организация Белорусский национальный технический университет

Защита состоится 19 ноября 2024 г. в 14.30 на заседании совета по защите диссертаций Д 01.04.01 при государственном научном учреждении «Объединенный институт проблем информатики НАН Беларуси» по адресу: 220012, г. Минск, ул. Сурганова, 6.

Телефон ученого секретаря: +375 17 378 21 46,
e-mail: eduard.snezhko@gmail.com.

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

Автореферат разослан 14 октября 2024 г.

Ученый секретарь
совета по защите диссертаций
кандидат технических наук, доцент



Э.В. Снежко

ВВЕДЕНИЕ

Развитие информационных систем и процессов привело к тому, что сейчас информация является одним из важнейших видов ценностей. Получение доступа к ней стало настолько простым, что несет угрозу нарушения безопасности, легитимности использования информационных ресурсов при отсутствии мер по их защите. То, что с одной стороны является товаром в цифровой форме, с другой – результат интеллектуального или творческого труда. Таким образом, возникла необходимость обеспечения защиты авторских прав на электронный контент. Цифровые произведения представлены во множестве компьютерных форматов, располагаются на мобильных, портативных и стационарных компьютерах и передаются по сети по различным протоколам. Зачастую для защиты авторских прав невозможно или чрезвычайно затруднено использование криптографических методов, и естественным подходом является применение стеганографических методов. В отличие от криптографии в стеганографии скрывается сам факт существования тайного сообщения. Именно такое тайное сообщение (или цифровой водяной знак, ЦВЗ) помогает не только устанавливать авторство, но и в определенной мере обеспечивает целостность защищаемого документа-контейнера.

Цифровая стеганография успешно развивается начиная с 1990-х гг.: проводятся конференции по проблеме сокрытия данных, разрабатываются методы и алгоритмы функционирования стеганографических систем. В последние годы появляются стеганографические методы, имеющие прикладную направленность: для встраивания информации в графические изображения, файлы различных форматов, объекты медиaprостранства. Значительное внимание уделяется вопросам емкости стегоконтейнера или пропускной способности стегаканала при сокрытии данных.

Для защиты авторских прав и подтверждения целостности цифровых объектов стеганографические методы используются довольно часто. Анализируемая предметная область подкреплена обширной библиографией. Однако в известных исследованиях стеганографическая система рассматривается как совокупность сообщений, файлов-контейнеров и методов по сокрытию сообщений в этих файлах, причем каждый тип объектов представляется как единый и неделимый. Зачастую же и контейнер, и сообщение могут быть представлены как набор связанных между собой компонентов. Например, электронные тексты в формате DOCX можно рассматривать также как набор файлов, основанных на языках разметки, а для сообщения можно вычислить контрольную сумму. Таким образом, к каждому из компонентов может применяться специфический стеганографический метод, и в каждый из компонентов может внедряться часть сообщения, и, таким образом ЦВЗ, внедряемые в эти компоненты, могут

использоваться для взаимного контроля. В той или иной степени подобный подход используют многие авторы, однако исследования компонентной модели стеганографической системы в известной литературе не представлено.

Современные информационные системы и реализуемые в них процессы характеризуются важными особенностями: на одной аппаратно-программной платформе могут интегрироваться модули, построенные на различных архитектурных принципах, с использованием различных языков программирования, библиотек и фреймворков. Для файлов, основанных на языках разметки (электронные географические карты (ЭК), текстовые документы, векторные изображения), имеющих значительное сходство структурного построения при существенном внешнем различии, могут быть разработаны обладающие большей емкостью как специфические, так и универсальные комплексные методы стеганографических преобразований этих документов для решения вышеозначенных задач. Однако из анализа доступной литературы следует, что существующие решения анализируемой научно-технической задачи не соответствуют современным требованиям. Все изложенное свидетельствует об актуальности темы диссертационного исследования и важности решения обозначенной задачи.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами, темами. Тема диссертационного исследования соответствует приоритетным направлениям научно-технической деятельности в Республике Беларусь на 2016–2020 гг. (Указ Президента Республики Беларусь от 22 апреля 2015 г. № 166 «О приоритетных направлениях научно-технической деятельности в Республике Беларусь на 2016–2020 годы») и 2021–2025 гг. (Указ Президента Республики Беларусь от 07 мая 2020 г. № 156 «О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021–2025 годы»).

Исследования проводились на кафедре информационных систем и технологий УО БГТУ в рамках НИР: ГПНИ «Информатика, космос и безопасность» 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» НИР ГБ 19-105 «Разработать стеганографические методы передачи информации в XML-документах, программные средства для реализации этих методов и методику оценки стеганоконтейнеров к взлому» (ГР № 20192461), ГПНИ «Цифровые и космические технологии, безопасность общества и государства» НИР ГБ 21-127 «Методы, алгоритмы и программные средства размещения невидимой идентификационной информации в электронных картах и

текстовых документах на основе стеганографии и избыточного кодирования» и опытно-конструкторской работы «Сборка, тестирование экспертной системы по реабилитации геологической среды, загрязненной нефтепродуктами, на основе принципов самоорганизации для территорий государств-участников СНГ и ее опытная эксплуатация», выполненной учреждением образования «Белорусский государственный технологический университет» в рамках договора № 11-1/8 от 8 июня 2017 г. с государственным предприятием «Научно-производственный центр по геологии».

Цель и задачи исследования. *Цель:* разработка и анализ новых эффективных стеганографических методов и реализующих их алгоритмов для решения задач защиты авторского права на электронные текстовые документы, изображения и ЭК, основанные на языках разметки, а также для обеспечения целостности этих документов.

Для достижения поставленной цели требуется решить следующие задачи.

1. Проанализировать текущее состояние проблемы охраны авторских прав на электронные текстовые документы, электронные изображения и ЭК, основанные на языках разметки, а также особенности использования стеганографических методов с целью обеспечения эффективного хранения и передачи тайной информации в компьютерных стеганографических системах.

2. Обосновать и разработать математическую модель компонентной стеганографической системы, предназначенной для защиты авторских прав на электронные текстовые документы, изображения и ЭК, основанные на языках разметки, и обеспечения целостности этих документов.

3. Разработать новые эффективные стеганографические методы, использующие компонентную модель, для электронных текстовых документов, изображений и ЭК, основанных на языках разметки.

4. Разработать алгоритмы размещения тайной информации в электронные документы на основе предложенных стеганографических методов для языков разметки, а также алгоритмы извлечения этой информации.

5. Разработать программные средства для реализации, анализа диапазона используемых параметров и эффективности использования разработанных стеганографических методов.

Объектом исследования является электронный контент в виде файлов на основе языков разметки. **Предметом** исследования выступают стеганографические методы, реализующие их алгоритмы и модели стеганографических преобразований, которые могут применяться для внедрения тайных данных в файлы, созданные на основе языков разметки.

Научная новизна полученных результатов:

1. Сформулирована и обоснована концепция компонентной стеганографической системы, отличающейся от известных систем представлением

контейнера, ключей и скрытого сообщения в виде набора связанных между собой компонентов, что позволяет более точно описать логические связи между компонентами системы и процессами, происходящими в ней.

2. Новизна разработанной математической модели стеганографической системы состоит в ее представлении в виде совокупности сообщений, файлов-контейнеров, многокомпонентного набора ключей, а также преобразований для разбиения контейнера на компоненты, сообщения – на блоки, вычисления контрольного значения, внедрения и извлечения сообщения, позволяющая учитывать использование различных ключей для скрытия блоков сообщения в разных компонентах.

3. В развитие предложенной концепции детализации и взаимосвязи компонентов стеганографической системы и математической модели ее описания обоснованы новые подходы в реализации такой системы, отличительные особенности которых заключаются в дополнении сообщения, осаждаемого в стегоконтейнер, блоком, представляющим собой определенным образом вычисленную контрольную сумму осаждаемого сообщения; поблочном разделении осаждаемого сообщения в соответствии с подобным секционированием исходного стегоконтейнера; многократном дублировании процедуры размещения сообщения в различных блоках стегоконтейнера.

4. В основу разработанных стеганографических методов и реализующих их алгоритмов положена идея использования дополнительных пространственно-геометрических параметров электронных текстовых документов, изображений и электронных карт, основанных на языках разметки, модификация которых позволяет скрывать тайную информацию для защиты авторского права и контроля целостности электронного контента.

Положения диссертации, выносимые на защиту.

1. Математическая модель компонентной стеганографической системы, представленной в виде совокупности разделенных на блоки сообщений, контейнеров, содержащих выделенные компоненты, трехуровневого ключа, а также преобразований для внедрения и извлечения тайного сообщения, характеризующаяся в сравнении с известными моделями более высокой степенью детализации, достигаемой за счет деления контейнера, ключа и сообщения на элементы, что обеспечивает возможность адаптации системы под решение узкоспециализированных задач.

2. Метод и алгоритмы прямого и обратного стеганографических преобразований информации на основе языков разметки, адаптированные к типу контейнера, отличающиеся тем, что встраиваемая в контейнер информация и ее контрольная сумма распределены по компонентам контейнера с учетом его параметров, что позволяет повысить емкость стеганографического контейнера не менее чем в 4 раза.

3. Стеганографический метод на основе встраивания дополнительных значений координат в географические электронные карты, позволяющий связать отдельные пространственные области для обеспечения целостности электронных карт, который отличается от других подобных методов тем, что связывает, по аналогии с концепцией блокчейн, пространственные области между собой, что обеспечивает более высокий уровень защищенности электронных карт от несанкционированной модификации.

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 научным руководителем.

Апробация результатов диссертации и информация об использовании ее результатов. Основные положения и результаты диссертационной работы были представлены на следующих научно-технических конференциях: 10-й МНТК “New Electrical and Electronic Technologies and their Industrial Implementation”, г. Закопане, Польша, 2015; 12–14 МНТК «Управление информационными ресурсами», Академия управления при Президенте Республики Беларусь, Минск, 2015–2017 гг.; Белорусско-Китайском молодежном инновационном форуме «Новые горизонты», Минск, 2017 г.; 17-й МНТК «Сахаровские чтения 2017 года: экологические проблемы XXI века», Минск, 2017 г.; V Международном Водном Форуме «Водные ресурсы и климат», Минск, 2017 г.; 4-й МНПК «Веб-программирование и интернет-технологии WeebConf 2018», БГУ, Минск, 2018 г.; 17-й МК «Развитие информатизации и государственной системы научно-технической информации (РИНТИ – 2018)», ОИПИ НАН РБ, Минск, 2018 г.; 6-й МНТК «Информационные технологии в образовании, науке и производстве», БНТУ, Минск, 2018 г.; 16-й Белорусско-российской НТК «Технические средства защиты информации», БГУИР, Минск, 2018 г.; 10-й МНТК «Информационные технологии в промышленности, логистике и социальной сфере (ITI*2019)», ОИПИ НАН РБ, Минск, 2019 г.; 19-й Белорусско-российской НТК «Технические средства защиты информации», БГУИР, Минск, 2021 г.; 8-й МНТК «Информационные технологии в образовании, науке и производстве», МИДО БНТУ, Минск, 2021 г.; 79–86 НТК профессорско-преподавательского состава, научных сотрудников и аспирантов, БГТУ, Минск, 2015–2023 гг.

Информация об использовании результатов. На основе предложенных в работе решений созданы и зарегистрированы в Национальном центре

интеллектуальной собственности Республики Беларусь 4 компьютерные программы, являющиеся импортозамещающими средствами, позволяющими практически реализовать скрытие и извлечение цифровых меток из электронных текстовых документов, изображений и электронных карт, основанных на файлах разметки. Результаты диссертационной работы внедрены и используются в Республиканском унитарном предприятии «Научно-производственный центр по геологии», а также в учебном процессе УО «Белорусский государственный технологический университет».

Опубликованность результатов. По результатам исследований опубликовано 36 печатных работ (8,2 а.л.), в том числе 8 статей в научных изданиях, входящих в Перечень ВАК Республики Беларусь, из которых 2 – на английском языке (Scopus), 16 статей в материалах конференций, тезисы 12 докладов, 4 свидетельства о регистрации компьютерных программ. Без соавторов опубликовано 7 работ.

Структура и объем диссертации. Работа состоит из введения, общей характеристики работы, 4 глав, заключения, списка использованных источников, включающего 119 наименований, списка публикаций соискателя, 3 приложений. Объем – 109 страниц, в том числе 44 иллюстрации, 17 таблиц.

ОСНОВНАЯ ЧАСТЬ

В первой главе проведен анализ современного состояния проблемы защиты авторского права на электронный контент, в частности защиты электронных текстовых документов, изображений и ЭК, выполненных на основе языков разметки (DOCX, SVG, SHP), от незаконного использования. Основной особенностью предметной области является небольшая емкость контейнеров по сравнению с растровыми изображениями и видео, поэтому важной является задача разработки методов, которые могут обеспечить внедрение в контейнер относительно небольших по объему данных, позволяющих защитить авторское право и проверить целостность объекта. Рассмотрены средства, реализующие стеганографические методы, отдельно или в комбинации с шифрованием. Предложена классификация применения стеганографических методов для электронных документов на основе языков разметки по признаку совместного использования. Перспективным направлением исследований представляется реализация стеганографических методов, которые разделяют ключевую информацию, внедряемое сообщение и стеганографический контейнер на части и используют это разделение для контроля целостности ЦВЗ.

Во второй главе сформулирована и обоснована концепция компонентной стеганографической системы, основанная на существующей математической модели, но отличающаяся представлением стеганографического

контейнера в виде набора компонентов, ключа в виде стегинонаборов, а скрываемого сообщения – в виде блоков. *Базовым ключом* называется такое конечное множество K^1 , $K^1 \subset K$, что существует такое преобразование F_1 , определенное на каком-либо подмножестве C_1 множества всех контейнеров C , что

$$F_1: C_1 \times K^1 \rightarrow S_1, \quad (1)$$

где S_1 – множество стегиноктейнеров, $S_1 \subset S$. Множество базовых ключей K^1 будем отождествлять с определенными особенностями стегинографического преобразования, реализуемыми для контейнеров C . *Ключом уровня контейнера* называется такое конечное множество K^2 , $K^2 \subset K$, что определено такое преобразование F_2 , что

$$F_2: K^2 \times C_2 \rightarrow S_2, \quad (2)$$

где S_2 – множество стегиноктейнеров, такое что $S_2 \subset S_1$. *Ключом уровня сообщения* называется такое конечное множество K^3 , $K^3 \subset K$, что существует такое преобразование F_3 , что

$$F_3: K^3 \times M \times C \rightarrow S_3, \quad (3)$$

где $S_3 \subset S$, M – множество сообщений.

Трёхуровневым ключом называется такое конечное множество K , которое представляет собой набор $\{K^1, K^2, K^3\}$, где K^1 – базовый ключ; K^2 – ключ уровня контейнера; K^3 – ключ уровня сообщения, такой, что для набора $\{C, M, K, S\}$ существует преобразование F , определенное на декартовом произведении множеств $M, C, \{K^1, K^2, K^3\}$, что

$$F: M \times C \times \{K^1, K^2, K^3\} \rightarrow S, \quad (4)$$

и может существовать такое преобразование F^{-1} , определенное на декартовом произведении S и K , что

$$F^{-1}: S \times \{K^1, K^2, K^3\} \rightarrow M, C. \quad (5)$$

Стегинонабором называется элемент $K = \{K^1, K^2, K^3\}$ множества ключей K , где ключи K^1, K^2, K^3 – базовый, уровня контейнера и сообщения соответственно.

Компонентом стегинографического контейнера C называется такое множество c , $c \subset C$, что для набора $\{c, M, S\}$, существует хотя бы один стегинонабор $\{K^1, K^2, K^3\}$, где K^1, K^2, K^3 – базовый ключ, ключ уровня контейнера и ключ

уровня сообщения соответственно, и существует преобразование f , такое, что

$$f: M \times c \times \{K^1, K^2, K^3\} \rightarrow S, \quad (6)$$

и может существовать такое преобразование f^{-1} , что

$$f^{-1}: S \times \{K^1, K^2, K^3\} \rightarrow M, c. \quad (7)$$

Преобразованием G , реализующим *выделение компонентов контейнера* из множества C , называется преобразование

$$G: C \rightarrow \{c_1, c_2, \dots, c_N\}, \quad (8)$$

где N – количество компонентов в множестве контейнеров C при разбиении G .

Блоком t скрытого сообщения M называется такая часть сообщения M , $M \subset M$, которая может быть скрыта в каком-либо компоненте c контейнера C с использованием стега набора K . Преобразованием H , реализующим *разбиение сообщения M на блоки*, называется преобразование

$$H: M \times \{c_1, c_2, \dots, c_N\} \rightarrow \{m_1, m_2, \dots, m_L\}. \quad (9)$$

Контрольным числом h для блока t скрытого сообщения M называется значение, рассчитанное путем применения определенного преобразования Z и используемое для проверки целостности блока t сообщения M . В качестве такого преобразования могут использоваться как функции (алгоритмы) хэширования, так и вычисление некоторой контрольной суммы.

Стеганографической системой \hat{S} называется совокупность, формально определяемая в следующем виде:

$$\hat{S} = (C, G, M, H, K, Z, F, F^{-1}), \quad (10)$$

где C – множество стегоконтейнеров, в которых выделены компоненты в соответствии с преобразованием G ; M – множество сообщений, состоящих из блоков, причем разбиение сообщения на блоки определяется преобразованием H ; K – множество стега наборов, состоящих из базовых ключей, ключей уровня сообщения и ключей уровня контейнера; Z – набор алгоритмов для вычисления контрольных чисел; F – функция сокрытия сообщения; F^{-1} – функция извлечения сообщения.

Обоснованы и описаны подходы использования предложенной математической модели компонентной стеганографической системы: проверка скрытого сообщения при помощи контрольного числа; разбиение сообщения на блоки и

сокрытие их в отдельных компонентах (рисунок 1а); последовательная проверка целостности скрытого сообщения на основе принципа блокчейн (рисунок 1б).

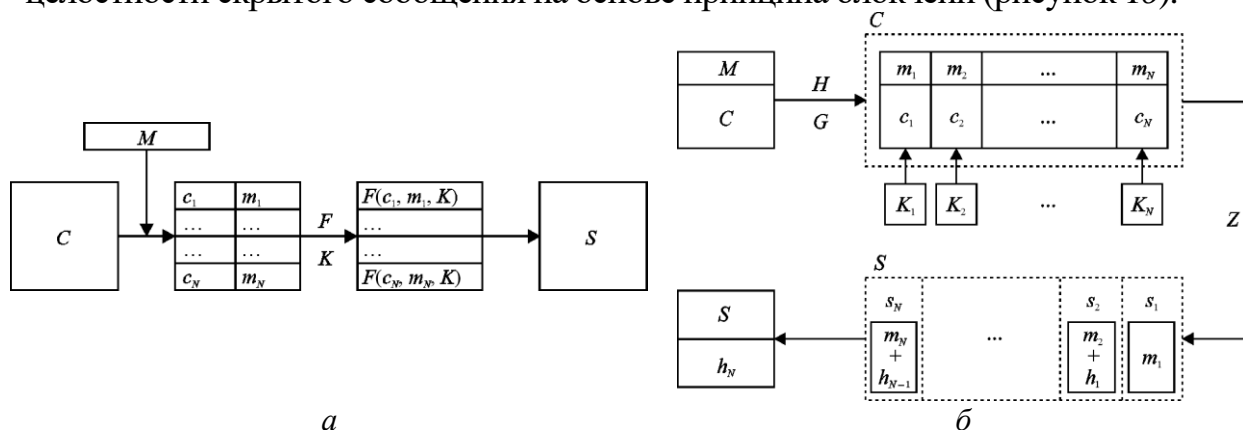


Рисунок 1 – Подход разделения сообщения на блоки и сокрытия их в отдельных компонентах (а) и подход последовательной проверки целостности скрытого сообщения на основе принципа блокчейн (б)

В третьей главе на основе модели компонентной стеганографической системы разработаны и описаны стеганографические методы, обеспечивающие взаимную зависимость между компонентами контейнера.

Метод *изменения межстрочного интервала неотображаемых символов* предназначен для размещения скрытых сообщений в файлах формата DOCX [1]. Предлагается производить смещение неотображаемых символов (пробелы, табуляции, знаки переноса строки и т. д.). Таким образом, емкость Δ метода может быть рассчитана как $\Delta = N_{\text{стр}} N_{\text{нс}} N_n$, где $N_{\text{стр}}$ – количество строк электронного документа, $N_{\text{нс}}$ – количество неотображаемых символов в каждой строке электронного документа, а N_n – количество разных позиций межстрочных интервалов. Пропускная способность Δ предложенного метода в $N_{\text{нс}}$ раз больше, чем пропускная способность Δ_0 известного метода (аналога) Line-Shift-Coding. Оценка пропускной способности основана на использовании вероятностных характеристик появления в текстах неотображаемых символов.

Разработан комбинированный подход, основанный на выделении компонентов c_1 (текст документа) и c_2 (разметка документа) стегоконтейнера C (файл DOCX) при применении стегонаборов K^1 (метод смещения неотображаемых символов) и K^2 (метод замены типа кавычек). Блок-схема алгоритма сокрытия сообщения и его контрольного значения изображена на рисунке 2. Метод изменения межстрочного расстояния для неотображаемых символов обозначен как *Spaces*, метод замены типа кавычек – как *Quotes*.

Емкость контейнера C для метода изменения межстрочного расстояния для неотображаемых символов обозначена как Δ_s , а емкость контейнера C для применения метода замены типа кавычек с двойных на одинарные – как Δ_Q . Сообщение M – бинарная последовательность длины L . Для M вычисляется

контрольное значение h – значение хеш-функции Z длиной l . Емкость Δ_S компонента c_1 стегоконтейнера C – количество всех пробелов. Емкость Δ_Q компонента c_2 стегоконтейнера C – количество пар кавычек в XML-разметке в файле *document.xml*, т. е. одна пара кавычек соответствует 1 биту скрытого сообщения. В зависимости от L и емкостей Δ_S и Δ_Q методы *Spaces* и *Quotes* могут быть использованы для разных компонентов контейнера.

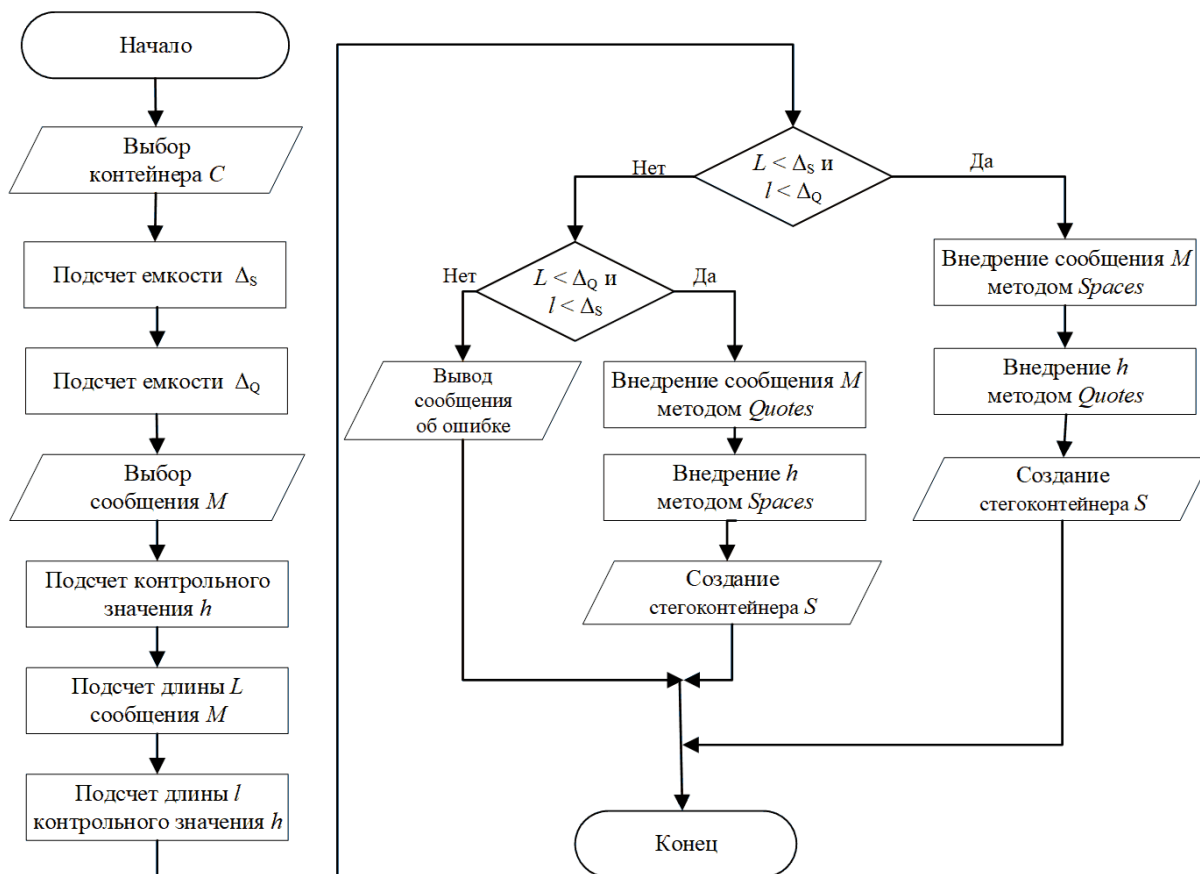


Рисунок 2 – Блок-схема алгоритма сокрытия сообщения и его контрольного значения

Данный подход может быть использован для размещения цифровых меток в файлы верстки электронных книг и журналов для выяснения канала несанкционированного копирования и распространения.

Обоснован и разработан стеганографический метод *дополнительных точек в кривые Безье*, позволяющий внедрять и извлекать скрытые сообщения при использовании в качестве контейнеров SVG-файлов [6]. Метод основан на добавлении дополнительных точек в кубические кривые Безье (КБ). Параметрическое уравнение КБ третьего порядка имеет следующий вид:

$$B(t) = (1 - t)^3 P_1 + 3(1 - t)^2 t P_2 + 3(1 - t) t^2 P_3 + t^3 P_4, t \in [0, 1]. \quad (11)$$

Для определения этой кривой потребуются четыре точки: P_1, P_2, P_3 и P_4 . На рисунке 3а показана КБ третьего порядка, которая состоит из трех сегментов, и ее описание в файле SVG, дополнительные линии отображают расположение контрольных точек; 3б – описание данной КБ.

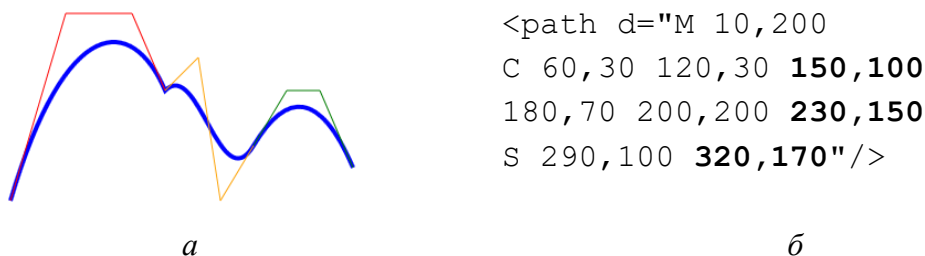


Рисунок 3 – Кривая Безье третьего порядка, состоящая из трех сегментов (а) и описание данной кривой Безье в файле SVG (б)

Согласно методу разбиения КБ, предложенному де Кастельжо, любую КБ можно разделить на две части в некотором отношении τ , причем полученные кривые будут также являться КБ. Координаты точек сегментов кривой могут быть вычислены из соотношения (11). При использовании следующих обозначений: $t_0 = 1 - \tau$; $t_1 = t_0^3$; $t_2 = 3 t_0^2 \tau$; $t_3 = 3 t_0 \tau^2$; $t_4 = \tau^3$, координаты точек $P_{11}(x_{11}, y_{11})$, $P_{12}(x_{12}, y_{12})$, $P_{13}(x_{13}, y_{13})$, $P_{14}(x_{14}, y_{14})$ кривой B_1 и координаты точек $P_{21}(x_{21}, y_{21})$, $P_{22}(x_{22}, y_{22})$, $P_{23}(x_{23}, y_{23})$, $P_{24}(x_{24}, y_{24})$ кривой B_2 могут быть вычислены по следующим формулам:

$$\begin{aligned}
 x_{11} &= x_1; y_{11} = y_1; & x_{21} &= x_{14}; y_{21} = y_{14}; \\
 x_{12} &= x_1 t_0 + x_2 \tau; y_{12} = y_1 t_0 + y_2 \tau; & x_{23} &= x_3 t_0 + x_4 \tau; y_{23} = y_3 t_0 + y_4 \tau; \\
 x_{13} &= x_{12} t_0 + (x_2 t_0 + x_3 \tau) \tau; & x_{22} &= x_{23} \tau + (x_2 t_0 + x_3 \tau) t_0; \\
 y_{13} &= y_{12} t_0 + (y_2 t_0 + y_3 \tau) \tau; & y_{22} &= y_{23} \tau + (y_2 t_0 + y_3 \tau) t_0; \\
 x_{14} &= x; y_{14} = y. & x_{24} &= x_4; y_{24} = y_4.
 \end{aligned}$$

Таким образом, исходная КБ B может быть представлена в виде двух сегментов: B_1 и B_2 , и записана в одном атрибуте d элемента $path$ в виде

$$\langle path d = "M x_{11}, y_{12} C x_{12}, y_{12} x_{13}, y_{13} x_{14}, y_{14} x_{22}, y_{22} x_{23}, y_{23} x_{24}, y_{24}" \rangle.$$

Основная сущность предлагаемого метода состоит в том, что для сокрытия информации используется местоположение точки разделения кривой на сегменты и разделение сообщения на блоки, представляющие собой бинарные пары $V_i, i = \{1, 2, 3, 4\}$. В качестве ключевой информации предлагается использовать два параметра: отношение разделения τ и значения Q_i , соответствующие бинарным парам $V_i, i = \{1, 2, 3, 4\}$. Исходная КБ разделяется в отношении τ или

$1 - \tau$ в зависимости от бинарной пары V_i , и в координаты опорных точек вносятся изменения δ_{ij} , где $\delta_{ij} = 10^{-6} q_{ij}$, так, что для опорных точек $P_{12}(x_{12}', y_{12}')$ и $P_{21}(x_{21}', y_{21}')$, показанных на рисунке 4, координаты вычисляются по формулам ниже слева или справа соответственно.

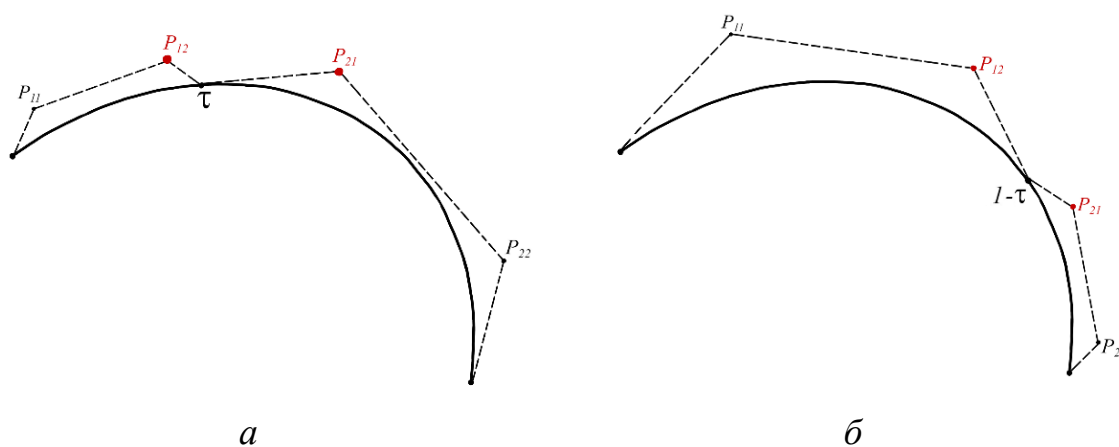


Рисунок 4 – Разделение кривой в отношении τ (а) и разделение кривой в отношении $1 - \tau$ (б)

$$x_{12}' = x_{12} + \delta_{11}, y_{12}' = y_{12} + \delta_{12};$$

$$x_{21}' = x_{21} + \delta_{21}, y_{21}' = y_{21} + \delta_{22}.$$

$$x_{12}' = x_{12} + \delta_{31}, y_{12}' = y_{12} + \delta_{32};$$

$$x_{21}' = x_{21} + \delta_{41}, y_{21}' = y_{21} + \delta_{42}.$$

Емкость Δ_B контейнера C для метода дополнительных точек в кривых Безье составит $\Delta_B = 4N$, где N – количество КБ, причем $\Delta_B > (L + l + 8)$, где L – длина сообщения M ; l – длина значения хеш-функции Z .

Обоснован и разработан метод *дополнительных секретных и контрольных вершин* для защиты авторского права и обеспечения целостности ЭК [8]. Предполагается, что у пользователя имеется ЭК в формате GeoJSON или Shapefile, в которой все объекты представлены в виде полигонов с набором дополнительных атрибутов, первый из которых (Id) является номером объекта. ЭК состоит из N пространственных объектов, $N > 2176$, каждый из которых обозначим как G_i , $i \in [1; N]$. Объект G_i является структурой и состоит из следующего набора полей: $(Id)_i$ – ключевой атрибут, номер G_i -го пространственного объекта; A_{i1}, \dots, A_{im} – дополнительные атрибуты G_i -го объекта электронной карты; g_i – описание исходной i -й пространственной области. ЭК рассматривается как последовательность полигонов в порядке атрибута Id . Пользователь формирует идентификатор I ; $I = \{D, O\}$; D – дата внедрения метки; O – данные о владельце ЭК. *Ключом первого рода* K_1 называется набор $\{D, O, N, H^1, H^2\}$, где H^1 – хеш-функция с длиной хэша 128 битов, H^2 – хеш-функция с длиной хэша 512 битов.

Для каждого полигона, начиная с первого, вычисляется h_i , обеспечивающее целостность данных в этом полигоне. Предлагается использовать в

качестве h_i шестнадцатеричное значение хеш-функции H^1 от конкатенации пространственного описания полигона g_i , его атрибутов A_{i1}, \dots, A_{im} , идентификатора пользователя $I = \{D, O\}$ и количества полигонов N , $h_i = H^1(g_i \parallel \{A_1, \dots, A_m\} \parallel I \parallel N)$, $i \in [1; N]$. Для сокрытия I необходимо преобразовать контрольное значение h_i к набору дополнительных вершин P_i , внедренных на ребра полигона g_i . Такой набор P_i полигона g_i называется *секретными вершинами*. При этом $h_i = \{h_{1i} h_{2i} \dots h_{32i}\}$, где h_{ji} – очередная цифра контрольного значения h_i в шестнадцатеричной системе счисления. Вершины P_i размещаются следующим образом: каждая вершина P_i устанавливается в отношении λ :

$$\lambda = \begin{cases} \frac{h_{ij}}{16}, & h_{ij} \neq 0 \\ \frac{1}{32}, & h_{ij} = 0 \end{cases}, \quad (12)$$

Необходимо случайным образом выбрать набор из 32 *секретных ребер* E_i пространственного объекта g_i , на которые будет осуществляться добавление вершин P_i для сокрытия каждого h_i . Для каждого полигона g_i генерируется список вершин P_i . На рисунке 5 показана установка части секретных вершин P_i на секретных ребрах E_i .

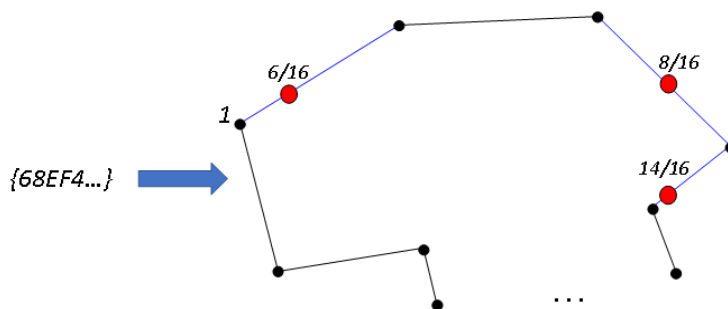


Рисунок 5 – Установка секретных вершин P_i в полигоне g_i

После установки вершин P_i описание пространственного объекта g_i изменится, новый объект обозначен как gs_i , а функция преобразования $F^{P_i}(g_i)$.

Для обратного преобразования необходимо узнать расположение набора секретных вершин P_i для извлечения идентификатора I из пространственного объекта gs_i . Для этого предлагается в следующий полигон ЭК (g_{i+1}) добавить еще один набор вершин R_i (здесь $i \in [2; N]$), из данных о расположении которых можно извлечь номера секретных ребер P_i , $i \in [1; N]$. Такие вершины R_i мы будем далее называть *контрольными вершинами*, а ребра T_i , на которых они установлены, – *контрольными ребрами*.

Расположение контрольных вершин \mathbf{R}_i должно быть известно автору ЭК. Предлагаем определять контрольные ребра \mathbf{T}_i полигона g_{i+1} как значение H_i хеш-функции H^2 от конкатенации идентификатора I и ключевого атрибута Id_i пространственного объекта $H_i = H^2(I \parallel N \parallel Id_i)$. Запишем H_i в виде $H_i = \{t_{1i}, t_{2i}, \dots, t_{128i}\}$, где t_{ji} – шестнадцатеричная цифра от 0 до F. Каждый набор контрольных ребер $\mathbf{T}_i, i \in [1; N]$, формируется следующим образом:

$$\mathbf{T}_i = \{t_{1i}, t_{1i} + t_{2i}, t_{1i} + t_{2i} + t_{3i}, \dots, t_{1i} + t_{2i} + \dots + t_{128i}\}. \quad (13)$$

Из полигона g_{si} известен набор вершин \mathbf{P}_i . Необходимо скрыть этот набор на контрольных ребрах \mathbf{T}_i . Поскольку не всегда номер секретной вершины \mathbf{P} является единичной цифрой, нужно отделить номера вершин друг от друга каким-либо символом. Для этого \mathbf{P}_i представляется в виде последовательности φ , причем вершины разделяются цифрой «0»

$$\varphi_i = [P_{1i} \ 0 \ P_{2i} \ 0 \ \dots \ 0 \ P_{32i}].$$

На контрольных ребрах \mathbf{T}_i в определенном отношении установлены контрольные точки $\mathbf{R}_i, i \in [2; N]$. Дополнительные точки \mathbf{R}_i в отношении устанавливаются от начала ребра по значению очередной цифры последовательности к числу 16, а если очередная цифра 0, то в отношении 1/32.

После установки контрольных вершин \mathbf{R}_i описание пространственного объекта g_{i+1} изменится. Обозначим описание нового пространственного объекта как g'_{i+1} , а функцию преобразования $\mathbf{F}^{\mathbf{R}_i}$:

$$\mathbf{F}^{\mathbf{R}_i}: g_{i+1} \rightarrow g'_{i+1}. \quad (14)$$

Для области g'_{i+1} выполняется преобразование $\mathbf{F}^{\mathbf{P}_{i+1}}$, в результате чего получаем пространственный объект $g_{s_{i+1}}$. Таким образом, каждый полигон g_i , кроме первого, проходит два преобразования: вначале $\mathbf{F}^{\mathbf{R}_i}$, при котором в полигон добавляются контрольные вершины \mathbf{R}_i , а затем $\mathbf{F}^{\mathbf{P}_i}$, при котором в полигон добавляются секретные вершины \mathbf{P}_i .

Первый полигон проходит только преобразование $\mathbf{F}^{\mathbf{P}_1}$. При этом секретные вершины \mathbf{P}_i полигона g_i записаны в текущем полигоне g_{s_i} , а его контрольные вершины \mathbf{R} – в следующем полигоне $g_{s_{i+1}}$, что позволяет последовательно связать все объекты ЭК наподобие системы блокчейн. После преобразования последнего полигона g_N получим полигон g_{s_N} :

$$\mathbf{F}^{\mathbf{R}_{N-1}}: g_N \rightarrow g'_N, \mathbf{F}^{\mathbf{P}_N}: g'_N \rightarrow g_{s_N}. \quad (15)$$

Для каждой пространственной области g_i последовательно выполняются

два преобразования:

$$F^P_1: g_1 \rightarrow g_{S1}; F^P_i: g'_i \rightarrow g_{Si}; F^R_{i-1}: g_i \rightarrow g'_i, i \in [2; N]. \quad (16)$$

После последовательного преобразования всех полигонов g_i пользователь получает ЭК с нанесенным идентификатором I и набор секретных вершин P_N , который называется *ключом второго рода* K_2 , $K_2 = \{P_{1N}, P_{2N}, \dots, P_{32N}\}$. Таким образом, все пространственные области g_i ЭК становятся последовательно связанными друг с другом, что позволяет защитить авторское право и контролировать целостность ЭК.

В четвертой главе описаны средства, в которых реализованы разработанные методы и алгоритмы. К ним относятся приложения, зарегистрированные в Национальном регистре интеллектуальной собственности Республики Беларусь: программный продукт *SpaceQuoteStego*, который может использоваться для сокрытия сообщения в файлах DOCX и позволяет контролировать целостность скрываемого сообщения; библиотека *StegoSVG*, позволяющая скрывать сообщения в файлах SVG, содержащих кубические КБ; набор процедур и функций базы данных для картографической информации в экспертной системе прогнозирования последствий разлива нефтепродуктов; интернет-сервис *StegoMap*, который позволяет скрывать ЦВЗ в файлах ЭК и проверять целостность ЭК на основе принципа блокчейн. Для программных средств был проведен анализ изменения размера файлов и времени генерации стегоконтейнеров, а также эксперимент по исследованию эффективности визуальных атак на стеганометоды. Результаты действия программных средств предлагались студентам 2–4-го курсов факультета информационных систем и технологий Белорусского государственного технологического университета. Итоги эксперимента показали, что обнаружение факта наличия внедренного в контейнер сообщения составляет 6,8% – для контейнеров формата DOCX, а раскрытие особенностей реализации стеганографической системы – 2,3%, для остальных типов контейнеров раскрытия особенностей реализации стеганографической системы не обнаружено. Таким образом, использование концепции компонентной стеганографической системы дает возможность успешно противостоять атакам с модифицированным контейнером и атакам подмены и/или имитации контейнера.

ЗАКЛЮЧЕНИЕ

Совокупность обоснованных в диссертационной работе положений, полученных научных и практических результатов позволяет решать актуальную, относящуюся к одному из приоритетных направлений научно-технической деятельности в Республике Беларусь задачу – защиты прав интеллектуальной собственности на электронный контент. В диссертации получены следующие теоретические и практические результаты:

1. Сформулирована и обоснована концепция компонентной стеганографической системы, основанной на ключевой информации в виде стегонаборов. Основным ее отличием от известных стеганографических систем является аналитическое представление стеганографического контейнера, ключевой информации и скрытого сообщения в виде наборов компонентов, уровней и блоков в зависимости от сферы применения, которая определяется типом используемого контейнера. Это позволяет определить логические связи между процессами, происходящими в такой системе, и структурой самой системы, что в конечном итоге упрощает программную реализацию стеганографических методов [4, 14, 19, 24, 34, 35].

2. Разработана математическая модель компонентной стеганографической системы, основанной на представлении ключевой информации в виде стегонаборов. Математической основой и отличительной особенностью модели является теоретико-множественное представление стеганографической системы как совокупности следующих множеств: компонентов стегоконтейнеров; преобразований, реализующих выделение компонентов контейнера; скрывааемых сообщений, состоящих из блоков; преобразований, реализующих разбиение сообщения на блоки; стегонаборов; преобразований, реализующих скрытие сообщения в стегоконтейнере и его извлечение, преобразований для вычисления контрольных чисел блоков сообщения. Определена взаимозависимость основных элементов математической модели, что позволяет описать стеганографическую систему более детально и точно [7, 10, 20, 23, 25].

3. Предложены новые подходы использования стеганографической системы, основанные на проверке целостности скрытого сообщения при помощи контрольного числа; разбиении сообщения на блоки и скрытии их в отдельных компонентах контейнера; последовательной проверке целостности скрытого сообщения на основе принципа блокчейн, что позволяет противостоять некоторым намеренным или случайным изменениям контейнера [5, 18, 23, 27, 29, 31, 33].

4. Обоснован и разработан стеганографический метод на основе изменения межстрочного интервала неотображаемых символов, который

отличается от известного метода большей емкостью (от 6 до 6,5 раз). Этот метод может быть использован в соответствии с концепцией компонентной стеганографической системы в комбинации с другим стеганографическим методом для защиты права собственности на электронный контент путем контроля целостности размещенных цифровых меток в файлы верстки электронных книг и журналов для выяснения канала несанкционированного копирования и/или распространения [1, 9, 26, 31].

5. Обоснован и разработан стеганографический метод, позволяющий внедрять и извлекать скрытые сообщения в контейнеры, являющиеся кубическими кривыми Безье в SVG-файлах, который отличается от известного подобного метода 4-кратно большей емкостью. В соответствии с концепцией компонентной стеганографической системы для сообщения может быть создан дополнительный блок, представляющий собой контрольное значение, что позволяет использовать данный метод для защиты прав интеллектуальной собственности на электронный контент в виде SVG-файлов [2, 6, 12, 17, 30].

6. Обоснован и разработан метод для обеспечения целостности электронных карт и защиты авторских прав на них, который основан на добавлении дополнительных секретных и контрольных точек в описании элементов пространственных областей с использованием схемы последовательного контроля целостности скрытого сообщения на основе принципа блокчейн. Метод может применяться путем нанесения ЦВЗ или цифровых меток на электронные карты, состоящие из областей, представляющих собой полигоны [8, 11, 13, 22, 28, 32].

7. В рамках разработанной экспертной системы прогнозирования последствий разлива нефтепродуктов приняты и внедрены в эксплуатацию стеганографический метод, алгоритм и процедуры для подтверждения авторства и целостности электронных карт в базе данных, позволяющий размещать скрытую информацию в расположении дополнительных точек в существующих полигонах, описывающих пространственные области электронных карт [3, 15, 16].

8. Разработаны и зарегистрированы в Национальном регистре интеллектуальной собственности Республики Беларусь программные средства на основе предложенных методов: программный продукт *SpaceQuoteStego*, библиотека *StegoSVG*, программный продукт *StegoMap* [4, 8, 17, 21, 30]. Результаты диссертационной работы внедрены и используются в Республиканском унитарном предприятии «Научно-производственный центр по геологии» и в учебном процессе УО «Белорусский государственный технологический университет».

Рекомендации по практическому использованию результатов

Результаты работы получены и реализованы в рамках госбюджетных НИР: ГБ 16-113, ГБ 19-105, ГБ 21-127, выполненных на кафедре информационных систем и технологий УО «Белорусский государственный технологический университет». На основе предложенных в работе решений могут быть сформулированы следующие рекомендации:

1. Разработанные стеганографические методы могут быть использованы не только для защиты права интеллектуальной собственности, но и для тайной передачи сообщений с возможностью контроля целостности.

2. Предложенная в работе концепция компонентной стеганографической системы, основанной на ключевой информации в виде стегаборонов, 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 исследования предложенных и похожих методов.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в научных рецензируемых изданиях из Перечня научных изданий Республики Беларусь для опубликования результатов диссертационных исследований

1. Блинова, Е. А. Стеганографический метод на основе изменения междустрочного расстояния неотображаемых символов строк электронного текстового документа / Е. А. Блинова // Труды БГТУ. – 2016. – № 6 (188). – С. 166–169.

2. Блинова, Е. А. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG / Е. А. Блинова, П. П. Урбанович // Труды БГТУ. – 2018. – № 1 (206). – С. 104–109.

3. Блинова, Е. А. Стеганографический метод на основе встраивания дополнительных значений координат в картографические данные / Е. А. Блинова // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2019. – № 1 (218). – С. 69–74.

4. Блинова, Е. А. Применение нескольких стеганографических методов для осаждения скрытых данных в электронных текстовых документах / Е. А. Блинова, А. А. Сущенья // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 32–38.

5. Сущенья, А. А. Математическая модель стеганографической системы с использованием стеганографического контейнера в виде электронной книги формата epub / А. А. Сущенья, Е. А. Блинова // Труды БГТУ. Серия 3: Физико-математические науки и информатика. – 2020. – № 1 (230). – С. 57–62.

6. Блинова, Е. А. Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG (Steganographic method based on hidden messages embedding into Bezier curves of SVG images) (на англ. языке) / Е. А. Блинова, П. П. Урбанович // Журнал Белорусского государственного университета. Математика. Информатика – 2022. – № 3. – С. 68–83.

7. Блинова, Е. А. Математическая модель стеганографической системы на основе ключевой информации в виде стегонаборов / Е. А. Блинова // Системный анализ и прикладная информатика. – 2022. – № 3. – С. 67–74.

8. Блинова, Е. А. Стеганографический метод для встраивания идентификатора в пространственные данные электронной карты (A steganographic method of embedding an identifier into the spatial data of an electronic map) (на англ. языке) / Е. А. Блинова, И. Ю. Шашевская, П. П. Урбанович // Журнал Белорусского государственного университета. Математика. Информатика – 2023. – № 1. – С. 76–87.

Статьи в сборниках материалов научных конференций

9. Shutko, N. The use of aprosh and kerning in text steganography / N. Shutko, E. Blinova // *New Electrical and Electronic Technologies and their Industrial Implementation; proceedings of the 9th Intern. Conf., Zakopane, Poland, 23–26.06.2015* / Lublin University of Technology; Media Patronage “Przeład Elektrotechniczny”. – Lublin, 2015. – P. 77.

10. Блинова, Е. А. Сравнительная оценка стеганографических методов в HTML-файлах / Е. А. Блинова // *Управление информационными ресурсами: материалы XII Междунар. науч.-практ. конф. Минск, 11 дек. 2015 г.* / Акад. упр. При Президенте Респ. Беларусь. – Минск, 2015. – С. 190.

11. Бурмакова, А. В. Реализация математической модели прогнозирования последствий аварийного пролива нефтепродуктов / А. В. Бурмакова, Е. А. Блинова, В. В. Смелов // *Новые горизонты – 2017 : сб. материалов Белорусско-Китайского молодежного инновационного форума, 2–3 ноября 2017 г. в 2 т.* / Белорус. нац. техн.ун-т. – Минск, 2017. – Т. 1. – С. 13–15.

12. Blinova, E. The use of steganographic methods in SVG format graphic files / E. Blinova, N. Shutko // *New Electrical and Electronic Technologies and their Industrial Implementation: Proceedings of the 10th Intern. Conf., Zakopane, Poland, 23–26 June 2017* / Lublin University of Technology; Media Patronage “Przeład Elektrotechniczny”. – Lublin, 2017. – P. 45.

13. Блинова, Е. А. Применение стеганографических методов при хранении картографической информации в экспертной системе прогнозирования последствий пролива нефтепродуктов / Е. А. Блинова, В.В. Смелов // *Сахаровские чтения 2017 года: экологические проблемы XXI века: материалы 17-й Междунар. науч. конф., Минск, 18–19 мая 2017 г. в 2 ч.* / Междунар. гос. экол. ин-т им. А. Д. Сахарова Бел. гос. ун-та; редкол.: С. Е. Головатый [и др.]; под ред. С. А. Маскевича, С. С. Позняка. – Минск, 2017. – Ч. 2. – С. 223–224.

14. Блинова, Е. А. Применение стеганографических методов для защиты данных электронных карт / Е. А. Блинова, П. П. Урбанович // *Управление информационными ресурсами: материалы XIV Междунар. науч.-практ. конф. Минск, 20 дек. 2017 г.* / Акад. упр. при Президенте Респ. Беларусь; под общ. ред. М. Г. Жилинского. – Минск, 2017. – С. 154–155.

15. Бурмакова, А. В. Реализация математической модели прогнозирования последствий аварийного пролива нефтепродуктов / А. В. Бурмакова, Е. А. Блинова, В. В. Смелов // *Управление информационными ресурсами: материалы XIV Междунар. науч.-практ. конф., Минск, 20 дек. 2017 г.* / Акад. упр. при Президенте Респ. Беларусь; под общ. ред. М. Г. Жилинского. – Минск, 2017. – С. 296–297.

16. Смелов, В. В. Экспертная система прогнозирования последствий

пролива нефтепродуктов / В. В. Смелов, Е. А. Блинова // Водные ресурсы и климат: материалы V Междунар. Водного Форума, Минск, 5–6 октября 2017 г. / Белорус. гос. технол. ун-т; редкол.: О. Б. Дормешкин [и др.] – Минск, 2017. – Ч. 1. – С. 196–197.

17. Блинова, Е. А. Модификация стеганографического метода на основе встраивания дополнительных значений координат в изображениях формата SVG / Е. А. Блинова, А. А. Голик // Развитие информатизации и государственной системы научно-технической информации (РИНТИ–2018): докл. XVII Междунар. конф., Минск, 20 сент. 2018 года. – Минск, 2018. – С. 130–133.

18. Колмаков, М. В. Программное средство для скрытия данных в альтернативных потоках файловой системы NTFS / М. В. Колмаков, Е. А. Блинова // Развитие информатизации и государственной системы научно-технической информации (РИНТИ–2018): докл. XVII Междунар. конф., Минск, 20 сент. 2018 года. – Минск, 2018. – С. 219–222.

19. Блинова, Е. А. Алгоритмические особенности и оценка эффективности использования стеганографических методов в электронных картах / Е. А. Блинова // Информационные технологии: материалы докл. 83-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с междунар. участием), Минск, 4–15 февраля 2019 г. / Белорус. гос. технол. ун-т. – Минск, 2019. – С. 33–35.

20. Блинова, Е. А. Алгоритмические особенности использования стеганографических методов в файлах, основанных на XML-разметке / Е. А. Блинова // Информационные технологии: материалы докл. 84-й науч.-техн. конф., посвященной 90-летию юбилею БГТУ и Дню белорусской науки (с международным участием), Минск, 03–14 февраля 2020 г. – Минск, 2020. – С. 30–31.

21. Блинова, Е. А. Приложение для нанесения стеганографического водяного знака на электронную карту / Е. А. Блинова, И. Ю. Сташевская // Информационные технологии в образовании, науке и производстве: материалы докл. VIII Междунар. науч.-техн. интернет-конф., 20–22 ноября 2021 г. / Междунар. ин-т дистанционного образования Белорус. нац. техн. ун-та (МИДО БНТУ), сост. Е. А. Хвилько. – Минск, 2022. – С. 193–198.

22. Блинова, Е. А. Использование формата GeoJson для нанесения стеганографического водяного знака на электронные карты / Е. А. Блинова, И. Ю. Сташевская // Информационные технологии: материалы докл. 86-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с междунар. участием), Минск, 31 янв. –12 февр. 2022 г. / Белорус. гос. технол. ун-т. – Минск, 2022. – С. 46–48.

23. Блинова, Е. А. Стеганографический метод на основе размещения

нескольких копий скрытого сообщения в SVG-контейнер / Е. А. Блинова, К. С. Марчук, П. П. Урбанович // Импортозамещение, научно-техническая и экономическая безопасность: сб. ст. V Междунар. науч.-техн. конф. «Минские научные чтения – 2022» в 3 т. Минск, 07–09 декаб. 2022 г. – Минск, 2022. – Т. 2. – С. 127–132.

24. Николайчук, А. Н. Комбинированное применение двух стеганографических методов для размещения цифрового водяного знака в файлах формата SVG / А. Н. Николайчук, Е. А. Блинова // Информационные технологии. Физика и математика: материалы докл. 87-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с междунар. участием), Минск, 31 янв. – 17 февр. 2023 г. / Белорус. гос. технол. ун-т. – Минск, 2023. – С. 57–60.

Тезисы докладов на научных конференциях

25. Блинова, Е. А. Классификация и сравнительная оценка методов текстовой стеганографии / Е. А. Блинова, П. П. Урбанович // Информационные технологии: тез. 79-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 2–6 февраля 2015 г. – Белорус. гос. технол. ун-т. – Минск, 2015. – С. 26.

26. Блинова, Е. А. Стеганографический метод на основе изменения межстрочного расстояния неотображаемых символов строк электронного текстового документа / Е. А. Блинова // Информационные технологии: тез. докладов 80-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с междунар. участием), 1–12 февр. 2016 г. / Белорус. гос. технол. ун-т; [гл. ред. И. М. Жарский]. – Минск, 2016. – С. 11.

27. Блинова, Е. А. Сравнительная оценка применимости стеганографических методов в графических файлах SVG / Е. А. Блинова, И. Г. Сухорукова // Информационные технологии: тез. докладов 81-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с междунар. участием), Минск, 1–12 февраля 2017 г. / Белорус. гос. технол. ун-т – Минск, 2017. – С. 17–18.

28. Блинова, Е. А. Защита целостности данных электронных карт стеганографическим методом / Е. А. Блинова, П. П. Урбанович // Веб-программирование и интернет-технологии (WebConf2018): тез. 4-й Междунар. науч.-практ. конф., Минск, 14–18 мая 2018 / Белорус. гос. ун-т. – Минск, 2018. – С. 147.

29. Блинова, Е. А. Стеганографическая система на основе комбинирования методов для электронного текстового документа / Е. А. Блинова, А. А. Сушня // Информационные технологии в образовании, науке и

производстве: тез. VI Междунар. науч.-техн. интернет-конф., 17–18 нояб. 2018 г. [Электронный ресурс]. – [Б. и.], 2018. – С. 2018. Режим доступа: <https://rep.bntu.by/handle/data/49869>. – Дата доступа: 02.09.2024.

30. Сущенья, А. А. Структура и описание программного средства реализующего стеганографическую систему на основе комбинирования методов для электронного текстового документа / А. А. Сущенья, Е. А. Блинова // Информационные технологии в образовании, науке и производстве: тез. VI Междунар. науч.-техн. интернет-конф., Минск, 17–18 ноября 2018 г. – Белорус. нац. техн. ун-т; сост. Е. В. Кондратёнок. – Минск, 2018. – С. 175–180.

31. Сущенья, А. А. Модификация стеганографического метода изменения междустрочного расстояния электронного документа / А. А. Сущенья, Е. А. Блинова, П. П. Урбанович // Технические средства защиты информации: тез. докл. XVI Белорусско-российской науч.-техн. конф., Минск, 5 июня 2018 г. – Белорус. гос. ун-т информатики и радиоэлектроники. – Минск, 2018. – С. 90.

32. Блинова, Е. А. Стеганографический метод на основе встраивания дополнительных значений координат в пространственные данные, хранящиеся в базе данных / Е. А. Блинова, П. П. Урбанович // Информационные технологии: тез. докл. 82-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 1–14 февр. 2018 г. / Белорус. гос. технол. ун-т. – Минск: БГТУ, 2018. – С. 8–9.

33. Колмаков, М. В. Особенности применения стеганографических методов в альтернативных потоках файловой системы NTFS / М. В. Колмаков, Е. А. Блинова // Информационные технологии: тез. докл. 82-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 1–14 февр. 2018 г. – Белорус. гос. технол. ун-т. – Минск, 2018. – С. 23–24.

34. Блинова, Е. А. Сравнительные особенности использования стеганографических методов в электронных картах / Е. А. Блинова, П. П. Урбанович // Информационные технологии в промышленности, логистике и социальной сфере (ИТИ*2019): тез. докл. X Междунар. науч.-техн. конф., Минск, 23–24 мая 2019 г. – Минск, 2019. – С. 22–24.

35. Блинова, Е. А. Стеганографический метод и приложение для размещения цифрового водяного знака в изображении формата SVG / Е. А. Блинова, П. П. Урбанович // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. – Белорус. гос. ун-т информатики и радиоэлектроники. – Минск, 2021. – С. 19.

36. Блинова, Е. А. Приложение для реализации стеганографической системы обмена сообщениями по протоколу ICMP / Е. А. Блинова, А. А. Бесман, П. П. Урбанович // Информационные технологии в промышленности,

логистике и социальной сфере (ІТІ*2023): тезисы докладов XII Междунар. науч.-техн. конф., Минск, 21–22 сентября 2023 г. – Минск, 2023. – С. 32–35.


Свидетельства о регистрации компьютерных программ

37. Экспертная система реабилитации геологической среды, загрязненной нефтепродуктами, на основе принципов самоорганизации для территории государств-участников СНГ: свид. о рег. компьютерной системы / Респ. унитарное предприятие «Научно-производственный центр по геологии»// Гос. рег. информационных ресурсов Респ. Беларусь. – 2019. – Запись № В-0157-01-2018 от 08.08.2018 г.

38. Блинова, Е. А. Библиотека «StegoSVG» для тайной передачи данных и защиты авторских прав на электронные векторные изображения формата SVG: свид. о рег. компьютерной программы / Блинова Е. А., Голик А. А. // Гос. рег. информационных ресурсов Респ. Беларусь. – 2022. – Запись № 1142228372 от 12.05.2022 г.

39. Блинова, Е. А. Прикладное программное средство «SpaceQuoteStego» для тайной передачи данных и защиты авторских прав на электронный контент формата .DOCX: свид. о рег. компьютерной программы / Блинова Е. А., Сушня А. А. // Гос. рег. информационных ресурсов Респ. Беларусь. – 2022. – Запись № 1142228356 от 12.05.2022 г.

40. Блинова, Е. А. Прикладное программное средство «StegoMap» для тайной передачи данных и защиты авторских прав на электронный контент формата Sharfile: свид. о рег. компьютерной программы / Блинова Е. А., Сташевская И. Ю. // Гос. рег. информационных ресурсов Респ. Беларусь. – 2022. – Запись № 1142228355 от 12.05.2022 г.



РЕЗЮМЕ

Блинова Евгения Александровна

Стеганографические методы и алгоритмы защиты авторского права и обеспечения целостности электронных документов на основе языков разметки

Ключевые слова: стеганография, языки разметки, стеганографическая система, электронный документ, векторное изображение в формате SVG, электронные карты.

Цель работы: разработка и анализ новых эффективных стеганографических методов и реализующих их алгоритмов для решения задач защиты авторского права на электронные текстовые документы, изображения и ЭК, основанные на языках разметки, а также для обеспечения целостности этих документов.

Методы исследования: исследования базируются на теории информационных процессов и систем, теории множеств, теории информации.

Полученные результаты и их новизна.

Сформулирована и обоснована концепция компонентной стеганографической системы, основанная на представлении ключевой информации в виде стега наборов. Разработана математическая модель компонентной стеганографической системы, стегоконтейнером которой могут быть файлы на основе языков разметки. Она представлена в виде совокупности сообщений, разделенных на блоки, файлов-контейнеров с выделенными компонентами, набора ключевой информации, а также преобразований для внедрения и извлечения сообщения. В основу разработанных методов положена идея использования дополнительных пространственно-геометрических параметров электронных документов, основанных на языках разметки, модификация которых позволяет скрывать тайную информацию для защиты авторского права и контроля целостности электронного контента.

Рекомендации по использованию и область применения.

Предложенная в работе концепция компонентной стеганографической системы может служить основой для расширения и углубления исследований по решению прикладных задач в предметной области, например при защите контента электронных образовательных средств.

РЭЗІЮМЭ

Блінова Яўгенія Аляксандраўна

Стэганаграфічныя метады і алгарытмы аховы аўтарскага права і забеспячэння цэласнасці электронных дакументаў на аснове моў разметкі

Ключавыя словы: стэганаграфія, мовы разметкі, стэганаграфічная сістэма, электронны дакумент, вектарны малюнак у фармаце SVG, электронныя карты.

Мэта работы: распрацоўка і аналіз новых эфектыўных стэганаграфічных метадаў і алгарытмаў, якія іх рэалізуюць, для вырашэння задач аховы аўтарскага права на электронныя тэкставыя дакументы, малюнкi і электронныя карты, заснаваныя на мовах разметкі, а таксама для забеспячэння цэласнасці гэтых дакументаў.

Метады даследавання: даследаванні праведзены з выкарыстаннем тэорыі інфармацыйных сістэм і працэсаў, тэорыі мностваў, тэорыі інфармацыі.

Атрыманыя вынікі і іх навізна.

Сфармулявана і абгрунтавана канцэпцыя кампанентнай стэганаграфічнай сістэмы, заснаваная на прадстаўленні ключавой інфармацыі ў выглядзе стэганабораў. Распрацавана матэматычная мадэль стэганаграфічнай сістэмы, стэгакантэйнерам якой могуць быць электронныя файлы, створаныя на аснове моў разметкі. Яна прадстаўлена ў выглядзе сукупнасці паведамленняў, падзеленых на блокі, файлаў-кантэйнераў, падзеленых на кампаненты, набору ключавой інфармацыі, а таксама стэганаграфічных пераўтварэнняў для утойвання і атрымання паведамлення. У аснову распрацаваных стэганаграфічных метадаў і алгарытмаў пакладзена ідэя выкарыстання дадатковых прасторава-геаметрычных параметраў і электронных карт, заснаваных на мовах разметкі, мадыфікацыя якіх дазваляе захоўваць тайную інфармацыю для аховы аўтарскага права і кантролю цэласнасці электроннага кантэнта.

Рэкамендацыі па выкарыстанні і галіна ўжывання.

Прапанаваная ў рабоце канцэпцыя кампанентнай стэганаграфічнай сістэмы, заснаваная на ключавой інфармацыі ў выглядзе стэганабораў, можа служыць метадычнай і інфармацыйнай асновай для пашырэння і паглыблення даследаванняў па вырашэнню задач у прадметнай галіне, напрыклад пры ахове кантэнта электронных адукацыйных сродкаў.

SUMMARY

Blinova Evgenia Aleksandrovna

Steganographic methods and algorithms for protecting copyright and ensuring the integrity of electronic documents based on markup languages

Keywords: steganography, markup languages, steganographic system, electronic document, vector image in SVG format, electronic maps.

Research objective: development and analysis of new effective steganographic methods and algorithms that implement them to solve problems of copyright protection for electronic text documents, images and electronic maps based on markup languages, as well as to ensure the integrity of these documents.

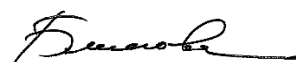
Research methods: research is based on the theory of information processes and systems, set theory, theory of information.

The results obtained and their novelty.

The concept of the component steganographic system based on the representation of key information in the form of stegosets is formulated and justified. A mathematical model of the component steganographic system has been developed, the stegocontainer of which can be files based on markup languages. It is presented in the form of a set of messages divided into blocks, container files with selected components, a set of key information, as well as steganographic transformations for embedding and extracting a message. The developed steganographic methods are based on the idea of using additional spatial and geometric parameters of electronic documents based on markup languages, the modification of which allows to hide secret information to protect copyright and control the integrity of electronic content.

Recommendations for use and application area.

The concept of a component steganographic system proposed in this work can serve as the basis for expanding and deepening research on solving applied problems in the subject area, for example, when protecting the content of electronic educational tools.



Научное издание

Блинова Евгения Александровна

**СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ И АЛГОРИТМЫ
ЗАЩИТЫ АВТОРСКОГО ПРАВА И ОБЕСПЕЧЕНИЯ
ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ
НА ОСНОВЕ ЯЗЫКОВ РАЗМЕТКИ**

Автореферат
диссертации на соискание ученой степени
кандидата технических наук
по специальности 05.25.05 – информационные системы и процессы

Ответственный за выпуск Е. А. Блинова

Подписано в печать 09.10.2024. Формат 60x84^{1/16}.
Бумага офсетная. Гарнитура Таймс. Печать ризографическая.
Усл. печ. л. 1,7. Уч.-изд. л. 1,8.
Тираж 60 экземпляров. Заказ 322.

Издатель и полиграфическое исполнение:
УО «Белорусский государственный технологический университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/227 от 20.03.2014.
Ул. Свердлова, 13а, 220006, г. Минск.