На правах рукописи



БЕЛОВА Ольга Александровна

ИНВАРИАНТНЫЕ СИСТЕМЫ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РЕАЛЬНОМ ВРЕМЕНИ ДЛЯ ЗВУКОВЫХ ПОКРЫВАЮЩИХ ОБЪЕКТОВ

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Самара – 2026

Работа выполнена на кафедре информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» (ФГБОУ ВО ПГУТИ)

Научный руководитель: доктор технических наук, доцент, заведующий кафедрой информационной безопасности ФГБОУ ВО ПГУТИ **Шакурский Максим Викторович**

Официальные оппоненты: **Бабенко Людмила Климентьевна**, доктор технических наук, профессор, профессор кафедры «Безопасность информационных технологий им. О.Б. Макаревича» федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет»

Гофман Максим Викторович, доктор технических наук, доцент, профессор кафедры «Информатика и информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения императора Александра I»

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики», г. Новосибирск.

Защита состоится «22» декабря 2026 г. в 10:00 часов на заседании диссертационного совета 24.2.479.07 на базе федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» по адресу: 450008, г. Уфа, ул. К. Маркса, д. 12.

С диссертацией можно ознакомиться в библиотеке федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» и на сайте: *https://uust.ru/*

Автореферат разослан «_____» октября 2026 г.

Ученый секретарь
диссертационного совета,
доктор технических наук Вульфин Алексей Михайлович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современные системы защиты информации все чаще функционируют в условиях потоковой передачи данных и их обработке в реальном времени. Аудиоинформация, широко используемая в телекоммуникационных, мультимедийных и управляющих системах, представляет собой перспективный, но недостаточно исследованный объект для использования в стеганографической защите. В отличие от изображений, звуковые сигналы обладают одномерной структурой и обрабатываются блочно, что накладывает дополнительные ограничения на применяемые методы сокрытия информации.

Существующие стеганографические методы звуковых покрывающих объектов, работающие в реальном времени, ориентированы на младшие битовые слои, обладающие известными статистическими свойствами, и не учитывают изменения статистических характеристик старших битовых слоев. Кроме этого, широко применяемые методы стегоанализа, основанные на дивергенции Кульбака-Лейблера и корреляционном анализе, оказываются недостаточно эффективными для выявления сложных зависимостей между битовыми слоями звуковых объектов.

В этой связи актуальной является разработка инвариантных стеганографических систем, адаптированных к особенностям звуковых сигналов и обеспечивающих повышенную скрытность передачи секретной информации в режиме реального времени.

Степень проработанности темы исследований. Проблемы цифровой стеганографии достаточно широко представлены в научных исследованиях, однако основное внимание уделяется изображениям и видеоданным. Значительный вклад в формирование теоретической и методологической базы исследований в области стеганографии внесли зарубежные ученые, такие как R. J. Anderson, W. Bender, C. Cachin, S. Craver, J. Fridrich, N. F. Johnson, N. Morimoto, B. Pfitzmann, I. Pitas, B. Schneier, G. J. Simmons, S. Voloshynovskiy. Среди отечественных исследователей необходимо отметить работы С. В. Белима, И. С. Вершинина, В. Г. Грибунина, Г. Ф. Конаховича, В. И. Коржика, И. Н. Окова, А. Ю. Пузыренко, В. А. Райхлина, Б. Я. Рябко, И. В. Туринцева, В. Н. Кустова, Л. К. Бабенко, В. В. Нечты, М.В. Шакурского, М.В. Гофмана и других ученых, активно занимающихся разработкой методов информационного сокрытия и оценки устойчивости стеганографических систем.

Проведенный обзор научных публикаций показывает, что наибольших результатов достигли исследования, направленные на сокрытие информации в изображениях. Существенный вклад в это направление сделан J. Fridrich, в чьих работах представлены подходы к реализации стеганографии в стационарных графических объектах. Однако с развитием цифровых коммуникаций и возрастанием объемов потоковой передачи информации наблюдается смещение интереса исследователей в сторону динамических медиаформатов. Особое внимание в последние годы стало уделяться

вопросам защиты информации, скрытой в аудиосреде. Начиная с 2020 года, в связи с массовым переходом к удалённой работе, дистанционному обучению и ростом популярности VoIP-технологий (видеосвязь, голосовые мессенджеры, онлайн-конференции), значительно увеличился обмен аудиосообщениями в реальном времени. Это вызвало повышенный интерес к разработке стеганографических методов, адаптированных к потоковой передаче голосовой информации. При этом следует заметить, что работы, посвященные стеганографии в звуковых сигналах, как правило, ограничиваются простыми методами замены младших битов и не учитывают многослойную структуру битовых представлений и их статистические взаимосвязи.

Вопросы адаптивного встраивания информации, использования многокомпонентных контейнеров и применения расширенных статистических методов анализа в реальном времени остаются недостаточно изученными, что определяет научную новизну и практическую значимость настоящего исследования.

Объектом исследования являются методы стеганографической защиты информации, скрытой в цифровых звуковых сигналах, обрабатываемых в реальном времени.

Предметом исследования являются методы и алгоритмы двухкомпонентного и многослойного встраивания информации в битовые слои звуковых покрывающих объектов, а также методы оценки их статистических свойств.

Целью диссертационной работы повышение эффективности двухкомпонентных стеганографических систем, работающих в реальном времени со звуковыми покрывающими объектами без сжатия, за счет использования многоуровневого встраивания с применением алгоритма статистической адаптации встраиваемой информации к покрывающему объекту.

Для достижения цели исследования поставлены и решены следующие задачи:

1. Разработать способ многоуровневого стеганографического встраивания информации в звуковой покрывающий объект с адаптацией встраиваемой информации к покрывающему объекту и алгоритмы его реализации;
2. Разработать комплекс математических моделей двухкомпонентных стеганографических систем для многоуровневого встраивания информации в покрывающий объект в реальном времени;
3. Разработать метод визуально-численной оценки свойств стеганографических систем, использующих звуковые покрывающие объекты без сжатия;
4. Выполнить исследование алгоритмов, реализующих разработанные математические модели, с помощью компьютерного моделирования и определить условия, при которых происходит статистическая адаптация встраиваемой информации к информации покрывающих объектов.

Методы исследования. Для выполнения поставленных задач применялись методы математического и численного моделирования, спектральный анализ, а также статистические подходы, включая корреляционный анализ, а также алгоритмы стеганографического скрытия информации.

Научная новизна полученных результатов:

1. Разработан способ многоуровневого стеганографического встраивания информации, *основанный* на использовании двухкомпонентного контейнера, *отличающийся* использованием нового алгоритма выбора логической функции связи компонент контейнера, *позволяющий* повысить маскировку встроенной информации за счет реализации адаптации встраиваемых компонент к статистическим свойствам покрывающего объекта в реальном времени.
2. Разработан комплекс математических моделей двухкомпонентных стеганографических систем для многоуровневого встраивания информации в покрывающий объект в реальном времени, *основанный* на использовании оконного встраивания двухкомпонентного контейнера в покрывающий объект, *отличающийся* последовательным встраиванием второй компоненты в слои покрывающего объекта с использованием алгоритмов определения логических функций связи компонент контейнера, *позволяющих* формализовать процесс подбора параметров и синтезировать новые структуры стеганографических систем.
3. Предложен метод визуально-численной оценки свойств стеганографических систем, *основанный* на NIST тестах битовых последовательностей на псевдослучайность, *отличающийся* тем, что проводится вычисление распределения результатов NIST тестов битовых последовательностей, *позволяющее* проводить визуальную и численную оценку статистических свойств стегосистем и звуковых покрывающих объектов.
4. Сформулированы условия, при которых происходит статистическая адаптация встраиваемой информации к информации покрывающих объектов, *основанные* на проведенном исследовании и компьютерном моделировании алгоритмов, реализующих разработанные математические модели, *отличающиеся* выбором функции связи встраиваемых компонент в зависимости от суммы значений выборки бит из старших битовых слоев покрывающего объекта, *позволяющие* реализовать стеганографические системы адаптирующиеся к статистическим свойствам покрывающего объекта в реальном времени.

Положения, выносимые на защиту:

1. Способ адаптивного многоуровневого стеганографического встраивания информации.
2. Комплекс математических моделей двухкомпонентных стеганографических систем для многоуровневого встраивания информации в покрывающий объект в реальном времени.

3. Метод визуально-численной оценки свойств стеганографических систем и покрывающих объектов.

4. Условия реализации адаптивных многоуровневых стеганографических систем встраивания информации.

Теоретическая значимость исследования заключается в развитии научных представлений о стеганографической передаче информации в аудиосреде за счет: разработки математических моделей процессов встраивания сообщений в условиях использования двухкомпонентных звуковых контейнеров; обоснования подхода к формированию контейнеров на основе условных функциональных связей между компонентами аудиосигнала; применения адаптированных статистических методов анализа (в том числе тестов NIST) для оценки скрытности и устойчивости встроенной информации, что расширяет инструментарий анализа стеганографических систем.

Практическая значимость результатов работы. Возможность использования разработанных алгоритмов и методик при создании систем скрытой передачи информации в аудиоканалах. Реализованные программные модели могут быть использованы в прикладных системах защиты информации, а также в научных и образовательных целях. Результаты исследования переданы для внедрения в профильные организации.

Связь с научными программами, темами, грантами. Исследования выполнялись в инициативном порядке и в рамках работы на конкурсе соискателей и молодых ученых на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики «Гранты ИБ МТУСИ» (МТУСИ, Москва, 2022 г.) – грант на 2022-2023 гг. Соглашение № 40469-16/2022-к от 30.06.2022 г.

Соответствие паспорту специальности. Результаты диссертационного исследования соответствует следующим пунктам паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность:

п. 10 Модели и методы оценки защищенности информации и информационной безопасности объекта.

п. 15 Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию соответствующих средств защиты информации и обеспечения информационной безопасности.

Апробация результатов диссертации: Основные результаты были апробированы на различных международных и Всероссийских конференциях, в том числе: XIX Международная научно-практическая конференция «Инновационные, информационные и коммуникационные технологии» (Сочи, 2022 г.); II Всероссийская научно-практическая конференция «Теория и практика обеспечения информационной безопасности» (МТУСИ, Москва, 2022 г.); XXX Российская научно-техническая конференция «Актуальные проблемы информатики, радиотехники и связи» (ПГУТИ, Самара, 2023 г.); X Международная заочная

научно-практическая конференция «Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT-2023) (ПВГУС, Тольятти, 2023); VI Всероссийская молодежная научно-практическая конференция с международным участием «Информационные технологии обеспечения комплексной безопасности в цифровом обществе» (Уфа, 2023 г.), III Всероссийская научно-практическая конференция «Теория и практика обеспечения информационной безопасности» (МТУСИ, Москва, 2023 г.), XXVI Международная научно-техническая конференция, Самара, 2024, XXXI Российская научно-техническая конференция, Самара, 2024, XI Международная заочная научно-техническая конференция ITRT-2024 (Тольятти, 2024), XXXII Российской научно-технической конференции. Самара, 2025 (ПГУТИ, Самара 2025 г.), XXVII и XXIII Международных научно-технических конференций. Уфа, 2025, XXXIII Российской научно-технической конференции. Самара, 2026 (ПГУТИ, Самара 2026 г.), XII Международная заочная научно-техническая конференция ITRT-2026 (Тольятти, 2026).

Публикации. По теме диссертационного исследования опубликовано 29 научных работ, в том числе 7 научных статей в рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией Российской Федерации (из них: 3 научных статьи К4), 1 научная статья в журнале, индексируемом в базах данных Web of Science и Scopus; 4 свидетельства о государственной регистрации программ для ЭВМ, получено 2 патента на изобретение, 15 работ в трудах международных и всероссийских конференций.

Реализация результатов работы. Результаты исследований внедрены в учебную программу кафедры информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», в ООО «Идентификация», ФГБОУ ВО «Поволжский государственный университет сервиса».

Личный вклад автора. Все результаты, изложенные в диссертации, включая программные реализации предложенных в работе алгоритмов, получены автором самостоятельно. Проработка цели и задачи, способов их решения и вариантов представления результатов осуществляется автором совместно с научным руководителем.

Структура и объем диссертации. Диссертация состоит из введения, 4 глав, заключения, списка литературы и 3 приложений. Текст исследования представлен на 209 страницах, включая 9 таблиц и 114 рисунков. Список литературы состоит из 110 источников.

ОСНОВНЫЕ ПОЛОЖЕНИЯ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, конкретизированы цель и задачи исследования, определены объект и предмет исследования, обоснованы новизна и практическая ценность выносимых на защиту результатов.

В первой главе рассмотрены теоретические и методические основы стеганографической защиты информации, скрытой в цифровых звуковых сигналах. Проведен анализ существующих форматов представления звуковых данных. В отличие от изображений звуковые сигналы характеризуются одномерной структурой битового представления и могут содержать один или несколько каналов, что принципиально влияет на способы сокрытия информации.

Проанализированы особенности обработки аудиоинформации в реальном времени. Показано, что обработка информации в реальном времени, в пределах допустимой временной задержки, ограничивает использование известных стеганографических методов, использующих анализ покрывающих объектов для повышения эффективности маскировки информации. Поставлена задача развития инвариантных систем стеганографической защиты информации в реальном времени. Концепция инвариантности стеганографической системы базируется на теории инвариантности академика Петрова Б.Н. и сформулирована в работах Шакурского М.В. Инвариантность стеганографической системы достигается использованием двухкомпонентного стеганографического контейнера и позволяет реализовать абсолютную инвариантность алгоритма извлечения сообщения от покрывающего объекта. Основным достоинством таких систем является возможность установки связи встраиваемой информации с покрывающим объектом в реальном времени и обеспечением последующего извлечения скрытой информации независимо от покрывающего объекта.

Проведена оценка эффективности традиционных статистических методов анализа стегосистем, включая дивергенцию Кульбака–Лейблера и коэффициент корреляции Пирсона, применительно к выявлению изменений в битовых слоях звуковых покрывающих объектов. Проанализированные методы не позволили выявить статистические зависимости при малых изменениях в покрывающих объектах, что обосновало применение расширенного статистического анализа.

Во второй главе разработаны алгоритмы и математические модели процессов встраивания сообщения в покрывающий объект и его извлечения из стеганографической системы. При построении моделей учтена специфика обработки данных в реальном времени, реализуемой в оконном режиме, что обусловило представление процесса встраивания информации в окно выборки отсчетов звукового покрывающего объекта.

Математическая модель подсистемы встраивания одного бита сообщения в один n-ный отсчет ПО (1):

$$\begin{cases} z1_n = f_1\left(x_n \setminus a_{x_{n0}}\right), \\ z2_n = f(u_n, z1_n) \\ a_{y_{ni}} = a_{x_{ni}}, i \in 1 \ldots N-1 \\ a_{y_{n0}} = z2_n \end{cases} \quad (1)$$

где $z1_n$ – первая компонента, которая определяется из всего массива бит отсчета, за исключением младшего бита, $z2_n$ – вторая (встраиваемая)

компонента, которая представляет собой функцию первой компоненты и маскируемого бита u_n.

На рисунке 1 представлена структурная схема алгоритма стеганографического встраивания одного бита сообщения.

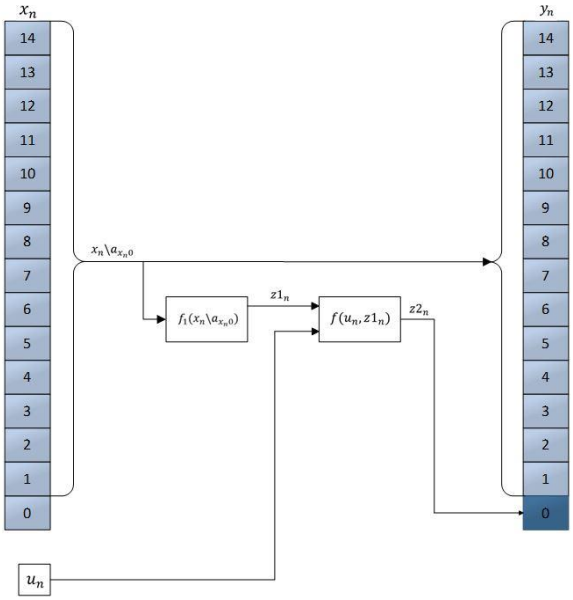


Рисунок 1 – Стеганографическая система, использующая встраивание одного бита сообщения в один *n*-ный отсчет ПО

Разработана математическая модель многослойного встраивания (2) информации, учитывающая использование модифицированного покрывающего объекта на каждой последующей итерации встраивания от старшего к младшему битовому слою.

$$\begin{cases} z1_{l,n} = f_1\left(x_{l,n} \setminus a_{x_n\, 0..L-l}\right), \\ z2_{l,n} = f(u_{l,n}, z1_{l,n}) \\ a_{y_n\, i} = a_{x_n\, i},\ i \in L \ldots N-1 \\ a_{y_n\, L-l} = z2_{l,n} \end{cases} \quad (2)$$

На рисунке 2 представлена структурная схема алгоритма стеганографического встраивания нескольких бит в пределах одного отсчета.

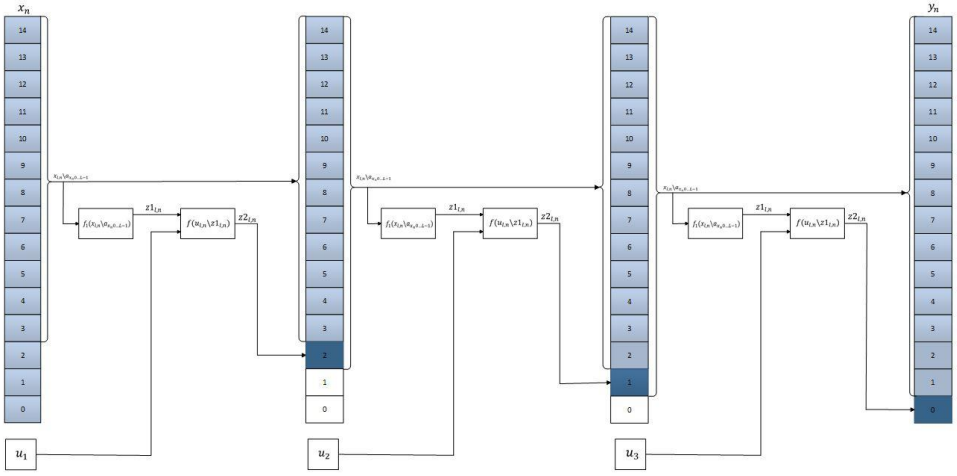


Рисунок 2 – Стеганографическая система, использующая многослойное встраивание нескольких битов сообщения в пределах одного отсчета

Поскольку обработка звуковых данных в реальном времени осуществляется в оконном режиме, разработана математическая модель стеганографической системы, реализующая встраивание двух компонент в пределах окна фиксированного размера (3).

$$\begin{cases} z1_{w,m} = f_1\left(x_{w,0..M-1} \setminus a_{xw,0..M-1\,0}\right), \\ z2_{w,m} = f(u_{w,m}, z1_{w,m}) \\ a_{y_{w,m\,i}} = a_{x_{w,m\,i}}, i \in 1 \ldots N-1 \\ a_{y_{w,m\,0}} = z2_{w,m} \end{cases} \quad (3)$$

В случае многослойного встраивания в пределах окна математическая модель является развитием модели многослойного встраивания (2) с учетом особенностей оконной обработки данных, описанных в (3), и имеет вид (4):

$$\begin{cases} z1_{l,w,m} = f_1\left(x_{l,w,0..M-1} \setminus a_{xl,w,0..M-1\,0..L-l}\right), \\ z2_{l,w,m} = f(u_{l,w,m}, z1_{l,w,m}) \\ a_{y_{w,m\,i}} = a_{x_{m\,i}}, i \in L \ldots N-1 \\ a_{y_{w,m\,L-l}} = z2_{l,w,m} \end{cases} \quad (4)$$

Разработан способ многослойного адаптивного встраивания информации в пределах окна. Способ стеганографической защиты информации основан на модификации бит покрывающего объекта, которые замещаются значениями, представляющими собой результат функции, применённой к биту сообщения и биту, выбранному по заданному алгоритму из старших разрядов двоичного представления отсчёта покрывающего объекта, функция, применяемая к каждому биту сообщения и каждому биту, выбранному из покрывающего объекта, выбирается каждый раз на основании значений выборки заданных бит старших разрядов покрывающего объекта, где под старшим разрядом подразумевается весь диапазон разрядов старше обрабатываемого в данный момент разряда, в случае если все значения выборки равны единице используется логическая функция ИЛИ, в случае, если все значения выборки равны нулю, используется логическая функция И, в остальных случаях используется логическая функция Исключающее ИЛИ, при этом если соотношение выбранного из старших разрядов покрывающего объекта бита и встроенного в стеганографическую систему бита при определённой алгоритмом логической функции не позволяет однозначно определить скрытый бит сообщения, выполняется его повторное встраивание в следующую позицию с новыми значениями выбранного бита из старших разрядов покрывающего объекта и новым определением логической функции, при этом используется блочная обработка отсчетов покрывающего объекта с размером блока, состоящим из заданного разработчиком количества отсчётов, причём каждый блок обрабатывается независимо от других, модифицируется определенное разработчиком количество младших разрядов отсчетов, начиная со старших модифицируемых разрядов выбранного блока отсчетов, и заканчивая самыми младшими разрядами.

Способ описывается математической моделью (5) с адаптивным механизмом выбора логической функции (И, ИЛИ, исключающее ИЛИ) в зависимости от статистического состава бит старших слоев покрывающего объекта. Такой подход позволяет снизить заметность модификации покрывающего объекта и адаптировать стеганографическую систему к изменяющимся характеристикам аудиосигнала.

$$\begin{cases} z1_{l,w,m} = a_{xk_{l,w,m}}, \\ z2_{l,w,m} = u_{l,w,m} \wedge z1_{l,w,m} \quad при\ c = 0 \\ z2_{l,w,m} = u_{l,w,m} \vee z1_{l,w,m} \quad при\ c = C \\ z2_{l,w,m} = u_{l,w,m} \oplus z1_{l,w,m} \quad в\ остальных\ случаях \\ a_{y_{w,m}\,i} = a_{x_{m}\,i},\ i \in L \ldots N-1 \\ a_{y_{w,m}\,L-l} = z2_{l,w,m} \end{cases} \tag{5}$$

где, c – сумма единичных бит из выборки заданного размера C, $\wedge$, $\vee$, $\oplus$ – логические функции И, ИЛИ, исключающее ИЛИ.

Пример процесса встраивания первого бита сообщения, в соответствии с моделью (5), представлен на рисунке 3.

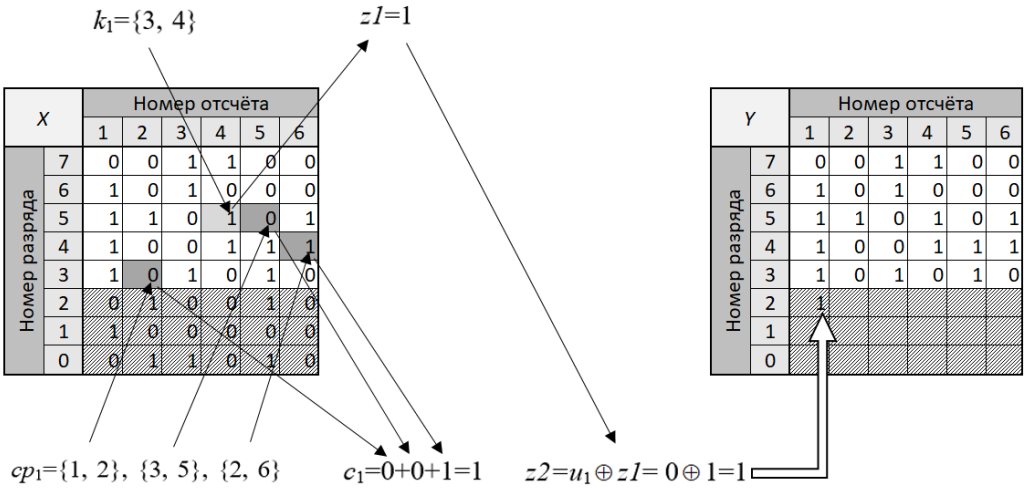


Рисунок 3 – Процесс встраивания первого бита сообщения

Рассмотрим процесс встраивания одного бита информации. Пусть бит данных u_1=0. В примере одному встраиваемому биту данных соответствует вектор из четырёх парных значений (координат), являющийся ключом системы. Первая пара значений k_1 определяет координаты первой компоненты двухкомпонентного контейнера, выбираемой из старших слоёв ПО $z1$=1. Три оставшихся пары значений cp_1 определяют координаты трёх точек выборки (в общем случае количество точек выборки может быть отличным от трёх). Сумма значений выборки трёх точек по координатам cp_1 представляет значение c_1=1. Для трёх точек c_1 может принимать значение от 0 до 3. Данное значение определяет используемую логическую функцию формирования второй компоненты. Если c_1=0, то используется функция И, если c_1=3, то используется функция ИЛИ, в остальных случаях (включая пример) используется функция Исключающее ИЛИ. Таким образом формирование второй компоненты происходит на основе выражения

$z2=u_1 \oplus z1= 0 \oplus 1=1$. Вторая компонента встраивается в ПО. Таким образом, поочерёдно происходит встраивание информации и формирование стегосистемы. Извлечение осуществляется в обратном порядке. Сперва определяется функция связи, затем первая компонента, затем бит встроенной информации.

В третьей главе демонстрируется разработанный метод визуально-численной оценки эффективности стеганографических алгоритмов. Метод основан на использовании статистического аппарата NIST тестов на случайность битовых последовательностей. Идея метода базируется на утверждении, что младший битовый слой звукового сигнала, снятого с аудиозаписывающих устройств, представляет собой случайную битовую последовательность, а тесты позволяют выявить закономерности, возникающие при модификации битовых слоев.

В соответствии с описанием каждый NIST тест возвращают параметр p, в случае, если он меньше 0,01 принимается решение о неслучайной последовательности бит. В предлагаемой методике пропускается данный этап, а результат вычисления p фиксируется в виде результата. Проверка битовой последовательности производится выбранным тестом, применяемым к скользящими окнам с определённым перекрытием. Полученный набор результатов p представляется в виде гистограммы из десяти корзин. Полученная гистограмма представляет собой визуализацию тестирования битовой последовательности. Численная оценка производится по амплитуде первого столбца гистограммы.

Рассмотрим пример анализа битовой последовательности. Последовательность сформирована из файла данных PDF, содержащего текст, формулы и рисунки. Данный документ использован в работе как источник данных встраиваемого сообщения. На рисунке 4 представлен результат тестирования фрагмента данных по 100 окнам с перекрытием.

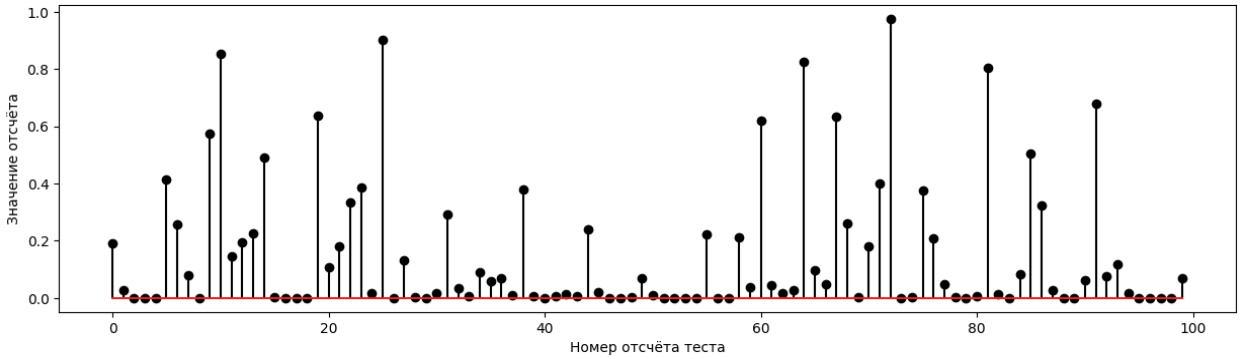


Рисунок 4 – Частотный побитовый тест (первый NIST тест) незашифрованных данных

Видно, что полученные результаты не обладают наглядностью. Сформируем гистограмму по полученным результатам (Рисунок 5). По амплитуде первого столбца можно сделать вывод, что большая часть тестов близка к «провалу». Рассмотрим результат тестирования битовых слоев звукового покрывающего объекта (рисунок 6). Видно, что в младшем

битовом слое амплитуды столбцов распределены равномерно, однако с повышением уровня амплитуда первого столбца растет, что говорит о большем количестве проваленных тестов и неслучайном характере последовательностей. Начиная с пятого слоя практически все тесты дают результат близкий к «провалу».

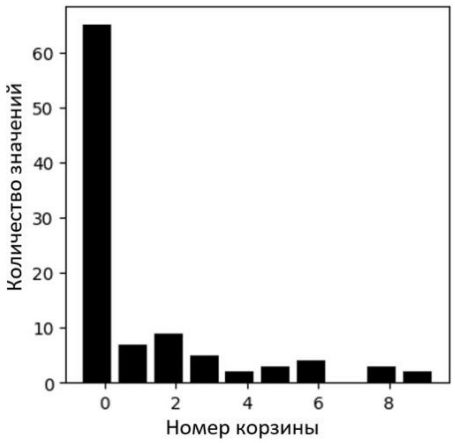


Рисунок 5 – Гистограмма результатов тестирования по 100 тестам

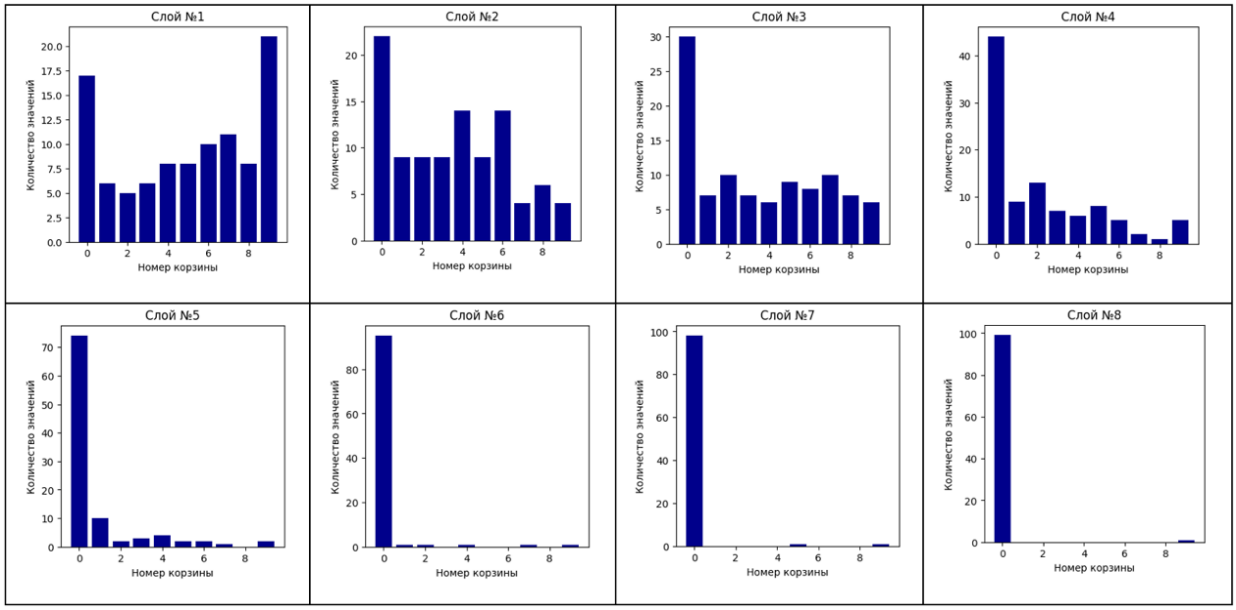


Рисунок 6 – Результаты тестирования битовых слоев покрывающего объекта

На рисунке 7 приведен график изменения амплитуды первой корзины от слоя. Чем выше значение графика – тем менее случайна последовательность (большое количество проваленных тестов). Данный инструмент визуализации позволяет оценить аномалии в статистических параметрах битовых слоев покрывающих объектов и стегосистем.

С целью всестороннего анализа результатов предложена модель сообщения в виде совокупности трех битовых последовательностей:

1. Исходной битовой последовательности, сформированной из PDF файла, содержащего текст, таблицы и рисунки;
2. Исходной последовательности, зашифрованной шифром AES
3. Исходной последовательности, зашифрованной шифром Кузнечик

Данный подход позволяет отойти от крайностей в тестовых данных (ярко выраженные особенности распределений значений) и приблизить результаты к реальным практическим ситуациям.

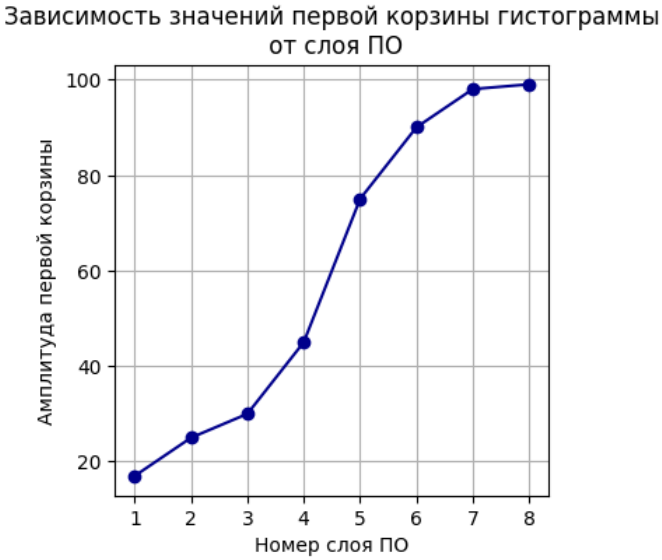


Рисунок 7 – Зависимость амплитуды первой корзины от слоя покрывающего объекта

В четвертой главе приведены результаты экспериментальных исследований и численное моделирование разработанных стеганографических алгоритмов. Моделирование всех разработанных алгоритмов встраивания, включая многоуровневое, а также вариант с адаптацией и без адаптации к статистическим характеристикам покрывающего объекта реализовано в среде Python. Разработанные алгоритмы зарегистрированы в качестве программ для ЭВМ.

Экспериментальные исследования выполнены для различных типов звуковых покрывающих объектов, представленных как в зашифрованном, так и в незашифрованном виде. Установлено, что применение многоуровневого встраивания более чем в два слоя приводит к статистически обнаружимым изменениям характеристик покрывающего сигнала (таблица 1).

Таблица 1 – Результаты тестирования первым тестом встраивания информации в один из музыкальных фрагментов

	Битовый слой	Сообщение	Встраивание без шифрования	Встраивание с шифрованием AES	Встраивание с шифрованием Кузнечиком
Уровень 3	48	29	21	12	24
Уровень 2	31	60	15	4	18
Уровень 1	26	51	5	10	16
Уровень 0 (младший)	14	29	13	4	15

Экспериментально установлено, что применение многоуровневого встраивания более чем в два слоя приводит к статистически обнаружимым изменениям покрывающего сигнала (рисунок 8).

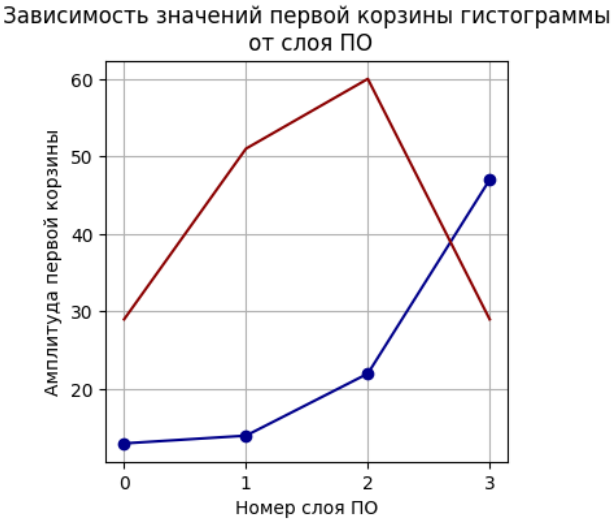


Рисунок 8 – Зависимость характеристик распределения результатов первого теста при многоуровневом встраивании от уровня битового слоя

Обоснована необходимость адаптации алгоритма встраивания к статистическим характеристикам покрывающего объекта посредством варьирования логических функций. Показано, что при использовании шифрования и двухкомпонентного контейнера встроенные данные обладают псевдослучайными свойствами, вследствие чего статистическая незаметность определяется преимущественно характеристиками покрывающего сигнала. Установлено, что обеспечение статистического сходства встроенных данных с покрывающим сигналом, в частности сохранение распределения, близкого к экспоненциальному, способствует снижению статистической обнаруживаемости стегосистемы (рисунок 9).

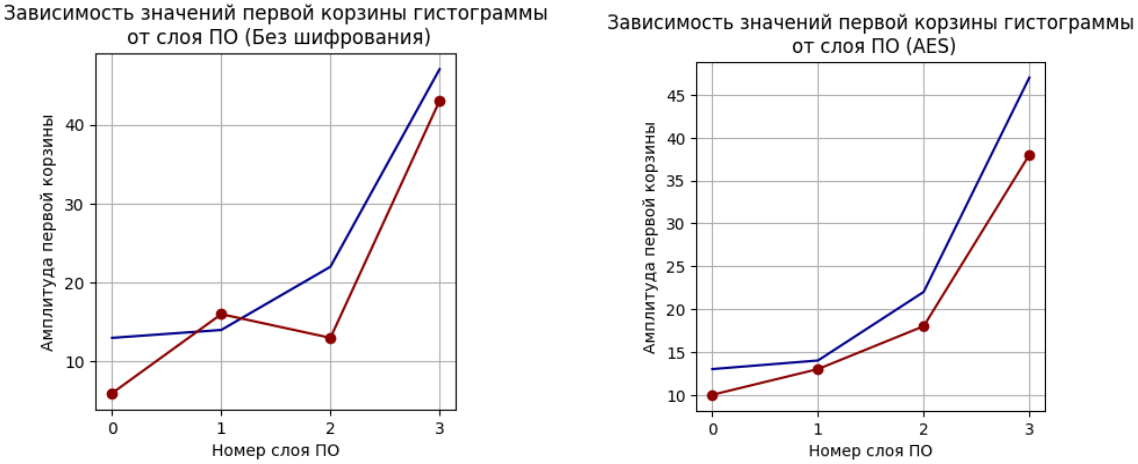


Рисунок 9 – Результат анализа стегосистемы без шифрования и с шифрованием AES

Эффективность разработанного адаптивного метода подтверждена результатами количественной оценки с использованием коэффициента корреляции Пирсона. Установлено, что применение адаптации обеспечивает коэффициент корреляции между статистическими распределениями покрывающего объекта и стегосистемы свыше 0,9, тогда как при отсутствии

адаптации его значение не превышает 0,4. Полученные результаты подтверждают эффективность предложенного метода с точки зрения обеспечения статистической маскировки (рисунок 10).

```
Коэффициент корреляции между результатами анализа ПО и бит сообщения -0.3768270800979498
Коэффициент корреляции между результатами анализа ПО и двухкомпонентной стегосистемы без шифрования 0.9555277701614135
Коэффициент корреляции между результатами анализа ПО и двухкомпонентной стегосистемы с шифрованием AES 0.997401828810882
```

Рисунок 10 – Анализ результатов моделирования коэффициента корреляции

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

В диссертационной работе в рамках проблемы защиты информации решены важные научно-технические задачи, повышающие эффективность защиты информации посредством цифровой стеганографии через разработку и реализацию алгоритма многоуровневого встраивания двухкомпонентного стеганографического контейнера звуковой покрывающий объект в реальном времени.

По итогам выполненных исследований сделан ряд выводов:

1. Разработан способ многоуровневого встраивания информации в звуковой покрывающий объект. Показано, что в младшем битовом слое звуковых объектов последовательность бит имеет случайный характер. В старших битовых слоях этот характер проявляется слабее. Предложенный способ учитывает изменение характера битовых последовательностей слоёв при многослойном встраивании сообщения. Для исследования характера битовых последовательностей стегосистем разработаны модели сообщения, представляющие собой три варианта битовых потоков: первый вариант представляет собой реальные данные, второй вариант – зашифрованные данные шифром AES, третий вариант – данные, зашифрованные шифром Кузнечик. Все шифры использовались в режиме счетчика Галуа.

2. Разработан комплекс математических моделей двухкомпонентных стеганографических систем для встраивания информации как в младший битовый слой, так и для многоуровневого встраивания:

- Математические модели стеганографической системы, использующей встраивание двух компонент в пределах одного отсчета с использованием функции исключающего ИЛИ.
- Математические модели стеганографической системы, использующей встраивание двух компонент в пределах окна фиксированного размера с использованием функции исключающего ИЛИ.
- Математические модели стеганографической системы, использующей встраивание двух компонент в пределах окна фиксированного размера с использованием условных функций определения второй компоненты стегоконтейнера.

3. Разработан метод визуально-численной оценки статистических свойств битовых последовательностей слоев звуковых потоков, использующий NIST тесты, которые применяются к скользящему окну выборки, с последующим построением гистограммы результатов

тестирования. В тестах порог определения случайности p=0.01, поэтому визуальная оценка делается по младшему столбцу гистограммы. Численным параметром оценки является величина младшего столбца гистограммы.

4. Разработаны компьютерные модели двухкомпонентных стеганографических систем в среде Python. Исследования, выполненные с помощью компьютерного моделирования, показали эффективность маскировки встраиваемой информации за счёт статистической адаптации двухкомпонентного стеганографического контейнера к параметрам покрывающего объекта. Определены условия, при которых происходит статистическая адаптация встраиваемой информации к информации покрывающих объектов. В результате применения предложенного алгоритма удалось повысить коэффициент корреляции между покрывающим объектом и стегосистемой до значения выше 0,9 против 0,38 между исходными данными.

Полученные научные и практические результаты позволяют повысить эффективность защиты встраиваемой информации с помощью инвариантных систем стеганографической защиты информации в реальном времени при использовании звуковых покрывающих объектов за счет повышения сокрытия и повышения сложности извлечения сообщения.

Перспективы дальнейшей разработки темы. Дальнейшее развитие темы диссертационного исследования планируется в трех направлениях:

1. Исследование встраивания двухкомпонентного контейнера в звуковые покрывающие объекты со сжатием, включая покрывающие объекты, сформированные на основе речевых кодеков;

2. Исследование возможности адаптации разработанной метода оценки стегосистем для проведения стегоанализа в реальном времени;

3. Исследование более сложных функций статистической адаптации двухкомпонентных стегосистем к покрывающим объектам.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях, рекомендованных Высшей аттестационной комиссией Российской Федерации

1. *Шакурский М.В.* Двухкомпонентная стеганографическая система на основе отношения линейных функций двух сигналов с размещением информативного сигнала в знаменателе функции встраивания сообщения / М.В. Шакурский, О.А. Караулова // Инфокоммуникационные технологии. – 2022. – Т. 20, № 1. – С. 118-124.

2. *Шакурский М.В.* Устойчивость двухкомпонентной стеганографической системы к несанкционированному извлечению информации / М.В. Шакурский, О.А. Караулова, Е.С. Карташевская // Проблемы информационной безопасности. Компьютерные системы. – 2022. – № 4(52). – С. 20-27.

3. *Шакурский М.В.* Оценка маскировки сигнала двухкомпонентной стеганографической системой при оконной обработке информации / М.В.

Шакурский, О.А. Караулова // Проблемы информационной безопасности. Компьютерные системы. – 2023. – № 2(54). – С. 9-16.

4. *Шакурский М.В.* Особенности использования NIST тестов для анализа битовых слоев покрывающих объектов в системах стеганографии / М.В. Шакурский, Н.И. Козырева, О.А. Караулова // Инфокоммуникационные технологии. – 2024. – Т. 22, № 3(87). – С. 41-48.

5. *Белова О.А.* Двухкомпонентная стеганографическая система, использующая многослойное оконное встраивание информации в звуковые покрывающие объекты / О. А. Белова // Проблемы информационной безопасности. Компьютерные системы. – 2026. – № 1(68). – С. 9-14.

6. *Белова О.А.* Метод адаптивного стеганографического встраивания в реальном времени для увеличения объема скрываемой информации при сохранении маскировки / О.А. Белова // Вопросы защиты информации. – 2026. – № 1(152). – С. 3-7.

7. *Шакурский М.В.* Выбор параметров двухкомпонентного адаптивного стеганографического встраивания / М.В. Шакурский, О.А. Белова // Вопросы защиты информации. – 2026. – № 2(153). – С. 3-7.

Публикации в ведущих зарубежных рецензируемых журналах, индексируемых в базах данных Web of Science и Scopus

8. *Shakurskii M.V.* Resistance of a Two-Component Steganographic System to Unauthorized Information Extraction / M.V. Shakurskii, O.A. Karaulova, E. S. Kartashevskaya // Automatic Control and Computer Sciences. – 2023. – Vol. 57, No. 8. – P. 862-867.

Свидетельства о регистрации электронных ресурсов

9. Свидетельство о государственной регистрации программы для ЭВМ № 2023610522 Российская Федерация. Программа реализации инвариантной системы стеганографической защиты информации в реальном времени с использованием двухкомпонентных контейнеров для звукового сигнала WAVE: № 2022685387: заявл. 21.12.2022: опубл. 11.01.2023 / М.В. Шакурский, О.А. Караулова.

10. Свидетельство о государственной регистрации программы для ЭВМ № 2025694027 Российская Федерация. Программа оконного встраивания скрываемой информации в младшие биты звукового покрывающего объекта с использованием двухкомпонентного стеганографического контейнера: заявл. 17.11.2025: опубл. 03.12.2025 / М.В. Шакурский, О.А. Белова.

11. Свидетельство о государственной регистрации программы для ЭВМ № 2025693867 Российская Федерация. Программа многослойного оконного встраивания скрываемой информации в биты звукового покрывающего объекта с использованием двухкомпонентного стеганографического контейнера: заявл. 17.11.2025: опубл. 02.12.2025 / М.В. Шакурский, О.А. Белова.

12. Свидетельство о государственной регистрации программы для ЭВМ № 2025693701 Российская Федерация. Программа многослойного оконного встраивания скрываемой информации в биты звукового покрывающего объекта с использованием двухкомпонентного стеганографического

контейнера и адаптивного выбора логических функций заявл. 17.11.2025; опубл. 01.12.2025 / М.В. Шакурский, О.А. Белова.

Патент на изобретение

13. Патент № 2815915 C1 Российская Федерация, МПК H04L 9/00. Способ сокрытия информации: № 2023108967: заявл. 10.04.2023: опубл. 25.03.2024 / М.В. Шакурский, В.Н. Козловский, О.А. Караулова.

14. Патент № 2859964 C1 Российская Федерация, МПК H04L 9/00. Способ сокрытия информации: заявл. 09.10.2025: опубл. 14.04.2026 / М. В. Шакурский, О. А. Белова

Публикации международных конференций

15. *Караулова О. А.* Особенности оценки стеганографических систем с точки зрения стеганографического анализа / О.А. Караулова, М.В. Шакурский // Инновационные, информационные и коммуникационные технологии: Сборник трудов XIX Международной научно-практической конференции, Сочи, 01–10 октября 2022 года / Под редакцией С.У. Увайсов. – Москва: Ассоциация выпускников и сотрудников ВВИА имени профессора Н.Е. Жуковского содействия сохранению исторического и научного наследия ВВИА имени профессора Н.Е. Жуковского, 2022. – С. 66-70.\

16. *Караулова О.А.* Особенности обеспечения безопасности данных с использованием сетевой стеганографии / О.А. Караулова, Н.В. Киреева // Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях: Материалы XXIV Международной научно-технической конференции и материалы XX Международной научно-технической конференции. В 2-х томах, Уфа, 23–25 ноября 2022 года. Том I. – Уфа: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уфимский университет науки и технологий", 2023. – С. 214.

17. *Шакурский М.В.* Стеганография в режиме реального времени / М.В. Шакурский, О.А. Караулова // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT-2023): Сборник тезисов докладов X Международной заочной научно-технической конференции, Тольятти, 20 апреля 2023 года / Редколлегия: В.И. Воловач (пред.) [и др.]. – Тольятти: Поволжский государственный университет сервиса, 2023. – С. 190-195.

18. *Караулова О.А.* Применение стеганографии для скрытой передачи информации в звуковых потоках в реальном времени / О.А. Караулова, М.В. Шакурский // VI Научный форум "Телекоммуникации: теория и технологии" ТТТ-2023: Материалы XXV Международной научно-технической конференции, Казань, 22–24 ноября 2023 года. – Казань: Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, 2023. – С. 106-107.

19. *Шакурский М.В.* Задача поиска скрытых сообщений в информационном потоке / М.В. Шакурский, О.А. Караулова // VII научный форум телекоммуникации: Теория и технологии ТТТ-2024: Материалы XXVI Международной научно-технической конференции, Самара, 06–08 ноября

2024 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2024. – С. 480-481.

20. *Шакурский М.В.* Задача поиска скрытых вложений в MIDI носителях / М.В. Шакурский, О.А. Караулова // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT- 2024): Материалы XI Международной заочной научно-технической конференции, Тольятти, 29 ноября 2024 года. – Тольятти: Издательско-полиграфический центр ПВГУС, 2025. – С. 78-81.

21. *Белова О.А.* Многоуровневое встраивание скрытой информации в цифровые звуковые объекты / О. А. Белова, М. В. Шакурский // Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях : материалы XXVII и XXIII Международных научно-технических конференций, Уфа, 05–07 ноября 2025 года. – Уфа: Уфимский университет науки и технологий, 2025. – С. 337-338.

22. *Белова О.А.* Метод визуального оценивания эффективности маскировки информации стегосистемой / О. А. Белова, М. В. Шакурский // Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях : материалы XXVII и XXIII Международных научно-технических конференций, Уфа, 05–07 ноября 2025 года. – Уфа: Уфимский университет науки и технологий, 2025. – С. 866-867

Публикации всероссийских конференций

23. *Караулова О.А.* Особенности использования стеганографии в звуке / О.А. Караулова, М.В. Шакурский // Теория и практика обеспечения информационной безопасности: сборник трудов II Всероссийской научно-практической конференции, Москва, 02 ноября 2022 года. – Москва: Без Издательства, 2022. – С. 14-21.

24. *Караулова О.А.* Особенности защиты информации в сетях передачи данных с использованием двухкомпонентных стеганографических систем / О.А. Караулова // Сборник трудов II Всероссийской научной школы-семинар. Современные тенденции развития методов и технологий защиты информации, МТУСИ, Москва, 2022. – С. 323-326.

25. *Караулова О.А.* Инвариантные стеганографические системы / О.А. Караулова, М.В. Шакурский // Актуальные проблемы информатики, радиотехники и связи: материалы XXX Российской научно-технической конференции, Самара, 28 февраля – 03 марта 2023 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2023. – С. 77-78.

26. *Караулова О.А.* Проблемы сокрытия информации в звуке, при его передаче в сети интернет в режиме реального времени / О.А. Караулова, М.В. Шакурский // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 26-29.

27. *Караулова О.А.* Исследование и разработка метода сокрытия информации в сетях передачи данных на основе инвариантных двухкомпонентных стеганографических систем / О.А. Караулова // Сборник трудов III Всероссийской научной школы-семинар. Современные тенденции развития методов и технологий защиты информации, МТУСИ, Москва, 2023. – С. 149-155.

28. *Шакурский М.В.* Стеганография в реальном времени / М.В. Шакурский, О.А. Караулова // Актуальные проблемы информатики, радиотехники и связи: Материалы XXXI Российской научно-технической конференции, Самара, 01–02 февраля 2024 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2024. – С. 115.

29. *Шакурский М.В.* Оценка маскировки в стеганографических системах / М.В. Шакурский, О.А. Караулова, С.З. Бильданов // Актуальные проблемы информатики, радиотехники и связи: Материалы XXXII Российской научно-технической конференции, Самара, 25–28 февраля 2025 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2025. – С. 99-101.

Диссертант  О.А. Белова